

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:

Application No.: 14/295,353

Filed: 06/04/2014

Applicant: Gurvinder Singh

Title: Automatic multimedia upload for
publishing data and multimedia content

Examiner: Nooristany, Sulaiman

Art Unit: 2415

Attorney Docket No.: Cellspin_04Con7_US

Mail Stop Amendment

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Amendment pursuant to 37 CFR § 1.312

Examiner Nooristany:

Please amend the above-referenced application as follows:

Amendments to the Claims are shown in the listing of claims which begin on page 2 of
this response.

Remarks begin on page 11 of this response.

Attachments:

1. Transmittal Form, PTO/SB/21.

Amendments to the Claims

Claim 1 (Currently Amended): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

~~sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device;~~

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;

receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;

enabling event notification on Bluetooth enabled data capture device, corresponding to new data;

determining existence of the new data for transfer; and

sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device;

encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and

transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely

identifies a particular user of internet service provided by the remote internet server.

Claim 2 (Original): The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

Claim 3 (Original): The method of claim 1, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Claim 4 (Original): The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 5 (Original): The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 6 (Previously Presented): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device;

determining existence of the new data for transfer; and

creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired;

encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device; and

transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination

web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.

Claim 7 (Original): The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

Claim 8 (Original): The method of claim 6, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Claim 9 (Original): The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 10 (Previously Presented): The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 11 (Previously Presented): The method of claim 6, wherein the time-stamp is either absolute time or relative time.

Claim 12 (Previously Presented): A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:

providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:

establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;

receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;

detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

 sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

 enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

 receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection;
and

sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key; and

transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

Claim 13 (Canceled):

Claim 14 (Previously Presented): The method of claim 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 15 (Previously Presented): The method of claim 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 16 (Previously Presented): A method for transferring data to a remoter internet server by a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled mobile device:

establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;

detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

 sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

 enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

 receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

 sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired;

receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;

obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key; and

sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

Claim 17 (Canceled):

Claim 18 (Previously Presented): The method of claim 16, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 19 (Previously Presented): The method of claim 16, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 20 (Previously Presented): The method of claim 6, wherein the time-stamp is either absolute time or relative time.

Remarks

The above referenced application has been allowed by the USPTO, as indicated in the Notice of Allowance mailed Oct 03, 2014.

Status of claims:

Claim 1 is currently amended.

Applicant would like to amend claim 1 prior to the payment of the issue fee for the above referenced application. The following limitation in claim 1 was inadvertently misplaced during an earlier communication to the Examiner:

"sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device".

Claim 1 as amended in this reply shows the correct placement of the above limitation. Applicant respectfully requests the Examiner to enter the above amendment since the above amendment is minor and does not change the scope of claim 1.

Accordingly, applicant respectfully requests that a timely "*Supplementary Notice of Allowance*" be issued for this application.

Conclusion

Applicant respectfully requests that the current amendment made pursuant to 37 CFR § 1.312 be considered. Applicant understands that an amendment after the notice of allowance is not a matter of right. However, applicant respectfully requests the recommendation of the primary examiner and approval of the Director, without withdrawing the application from issue. If Examiner Nooristany finds that a telephonic

conference will expedite the prosecution, the examiner is requested to schedule a telephonic conference with the undersigned using below contact information.

Respectfully submitted,

Date: Oct 09, 2014

/s tankha/
Ashok Tankha
Attorney For Applicant
Lipton, Weinberger & Husick
Reg. No. 33,802

Correspondence Address

Lipton, Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Fax: 856-374-0246
Phone: 856-266-5145
Email: ash@ipprocure.com



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

7590
ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

10/03/2014

EXAMINER

NOORISTANY, SULAIMAN

ART UNIT

PAPER NUMBER

2415

DATE MAILED: 10/03/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/295,353	06/04/2014	Gurvinder Singh	CellSpin_04Con7_US	9544

TITLE OF INVENTION: Automatic Multimedia Upload For Publishing Data And Multimedia Content

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	01/05/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. **PROSECUTION ON THE MERITS IS CLOSED.** THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN **THREE MONTHS** FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. **THIS STATUTORY PERIOD CANNOT BE EXTENDED.** SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

7590 10/03/2014
ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/295,353	06/04/2014	Gurvinder Singh	CellSpin_04Con7_US	9544

TITLE OF INVENTION: Automatic Multimedia Upload For Publishing Data And Multimedia Content

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	01/05/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
NOORISTANY, SULAIMAN	2415	709-232000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
☐ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____
Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/295,353	06/04/2014	Gurvinder Singh	CellSpin_04Con7_US	9544
7590 ASHOK TANKHA 36 GREENLEIGH DRIVE SEWELL, NJ 08080			EXAMINER	
			NOORISTANY, SULAIMAN	
			ART UNIT	PAPER NUMBER
			2415	
DATE MAILED: 10/03/2014				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/295,353	Applicant(s) SINGH ET AL.	Examiner SULAIMAN NOORISTANY	Art Unit 2478	AIA (First Inventor to File) Status No
-------------------------------	--------------------------------------	-------------------------------------	--	-------------------------	--

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/5/14, 9/23/14.
☐ A declaration(s)/affidavit(s) under 37 CFR 1.130(b) was/were filed on ____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-12, 14-16 and 18-20. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date ____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material 4. ☒ Interview Summary (PTO-413), Paper No./Mail Date <u>9/23/14</u> .	5. ☐ Examiner's Amendment/Comment 6. ☐ Examiner's Statement of Reasons for Allowance 7. ☐ Other ____
--	---

/SULAIMAN NOORISTANY/ Primary Examiner, Art Unit 2478	
--	--

The present application is being examined under the pre-AIA first to invent provisions.

Examiner Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ashok Tankha (Reg. # 33,802) on 9/23/2014.

Claims Are Amended As Follows:

CLAIMS:

Claim 1 (Currently Amended): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device;

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;

receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;

enabling event notification on Bluetooth enabled data capture device, corresponding to new data;

determining existence of the new data for transfer;
and

sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event

notification sent from the Bluetooth enabled data capture device; [[and]]

encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and

transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data [[.]] and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method. [[and]] wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.

Claim 2 (Original): The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

Claim 3 (Original): The method of claim 1, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Claim 4 (Original): The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 5 (Original): The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 6 (Currently Amended): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications

correspond to existence of new data for transfer on the Bluetooth enabled data capture device;

determining existence of the new data for transfer;
and

creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired; [[and]]

encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device;
and

transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object[[.]] and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises

one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, [[and]] wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.

Claim 7 (Original): The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

Claim 8 (Original): The method of claim 6, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Claim 9 (Original): The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 10 (Previously Presented): The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 11 (Previously Presented): The method of claim 6, wherein the time-stamp is either absolute time or relative time.

Claim 12 (Currently Amended): A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:

providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:

establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;

receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;

detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device,

over the established paired secure Bluetooth connection;

receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key; and

transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

Claim 13 (Canceled):

Claim 14 (Previously Presented): The method of claim 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 15 (Previously Presented): The method of claim 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 16 (Currently Amended): A method for transferring data to a remoter internet server by a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled mobile device:

establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;

detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired_secure Bluetooth connection;

receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired;

receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;

obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key; and

sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer

protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

Claim 17 (Canceled):

Claim 18 (Previously Presented): The method of claim 16, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 19 (Previously Presented): The method of claim 16, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 20 (Previously Presented): The method of claim 6, wherein the time-stamp is either absolute time or relative time.

Allowable Subject Matter

Claims 1-12, 14-16, 18-20 are allowed.

The following is a statement of reasons for the indication of allowable subject matter:

None of the prior art of the record explicitly teaches or fairly suggests all of the claimed limitation, especially the limitation wherein performing at a Bluetooth enabled data capture device: establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key; acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established; sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device; detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises: receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection; receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection; enabling event notification on Bluetooth enabled data capture device, corresponding to new data; determining existence of the new data for transfer; and sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device; encrypting, using cryptographic

encryption key, the new data acquired in the Bluetooth enabled data capture device; and transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data[.,] and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is (571) 270-1929. The examiner can normally be reached on M-F from 9 to 5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Derrick Ferris, can be reached on (571) 272-3123. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 14/295,353
Art Unit: 2478

Page 4

/SULAIMAN NOORISTANY/

Primary Examiner, Art Unit 2478

TERMINAL DISCLAIMER TO OBTAIN A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) CellSpin_04Con7_US
In re Application of: Gurvinder Singh, Marcos Klein and Vince Laviano Application No.: 14/295,353 Filed: 06/04/2014 For: Automatic Multimedia Upload For Publishing Data And Multimedia Content The owner*, CellSpinsoft Inc., of <u>100</u> percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number <u>14295352</u>, filed <u>04 June 2014</u>, as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns. In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that: any such patent: granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant. Check either box 1 or 2 below, if appropriate. 1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon. 2. ☒ The undersigned is an attorney or agent of record. Reg. No. <u>33802</u> _____ /s/ tankha/ Signature _____ Ashok Tankha Typed or printed name 07 August 2014 Date 856-266-5145 Telephone Number ☐ Terminal disclaimer fee under 37 CFR 1.20(d) is included. WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. *Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this statement. See MPEP § 324.	

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Application Number 	Application/Control No.	Applicant(s)/Patent under Reexamination	
	14/295,353	SINGH ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 07 AUG 2014	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:	
JAB	

U.S. Patent and Trademark Office

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:

Application No.: 14/295,353

Filed: 06/04/2014

Applicant: Gurvinder Singh

Title: Automatic Multimedia Upload
For Publishing Data And Multimedia
Content

Examiner: Nooristany, Sulaiman

Art Unit: 2478

Att. Docket No.: CellSpin_04Con7_US

Mail Stop Amendment

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Response to Office Action

Examiner Nooristany:

In response to the non-final office action dated July 08, 2014, please consider the amendment and remarks submitted in this response:

Amendment to the Claims is presented on page 2 of this response.

Remarks begin on page 11 of this response.

Attachments:

1. Transmittal Form, PTO/SB/21; and
2. Terminal disclaimer, Form PTO/SB/25;
3. Payment of the following fee:
-\$160 for the terminal disclaimer;

The Director is hereby authorized to charge any underpayment of fee or any other fee that may be required to deposit account # 503291.

Amendment to the Claims

We claim:

Claim I (Currently Amended): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server ~~one or more remote internet servers~~ via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device,
wherein the paired secure Bluetooth connection uses cryptographic encryption key;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;

receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;

enabling event notification on Bluetooth enabled data capture device, corresponding to ~~change in~~ new data;

determining existence of the new data for transfer; and

sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device; and

encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device;

transferring the ~~[[new]]~~ encrypted data ~~from acquired in~~ the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted ~~[[new]]~~ data, obtain the new data from the encrypted data using cryptographic encryption key, and send ~~[[it]]~~ the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server to one or more remote internet servers.

Claim 2 (Original): The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

Claim 3 (Original): The method of claim 1, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Claim 4 (Original): The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 5 (Original): The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 6 (Currently Amended): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server ~~one or more remote internet servers~~ via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for ~~event~~ data signal notifications, wherein the data signal

~~notifications correspond~~ corresponding to existence of new data for transfer[[.]] on the Bluetooth enabled data capture device;

~~determining existence of the new data for transfer;~~ and

~~creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal~~ notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer; and

~~sending an event notification to the Bluetooth-enabled mobile device, corresponding to existence of new data for transfer, over the established paired Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth-enabled data capture device;~~

encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device;

transferring the encrypted [[new]] data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted [[new]] data object, obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, and send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet

service provided by a remote internet server and time-stamp to one or more remote internet servers.

Claim 7 (Original): The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

Claim 8 (Original): The method of claim 6, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Claim 9 (Original): The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 10 (Currently Amended): The method of claim 6, wherein ~~event~~ said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 11 (Original): The method of claim 6, wherein the time-stamp is either absolute time or relative time.

Claim 12 (Currently Amended): A method for transferring data to a remote internet server ~~one or more remote internet servers~~ by a Bluetooth enabled mobile device comprising:

providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:

establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;

detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device[[,]] corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

receiving, ~~the new data~~ by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key[[,]]; and

transferring the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server~~received from the Bluetooth enabled data capture device to one or more remote internet servers.~~

Claim 13 (Currently Amended): The method of claim ~~[[11]]~~ 12, wherein the Bluetooth enabled mobile device configures the new data so that it can be received by a remote internet server~~one or more remote internet servers~~, and wherein configuring new data for receipt by a remote internet server~~one or more internet servers~~ comprises specifying action setting and destination address of ~~[[the]]~~ a remote internet server ~~one or more internet servers~~.

Claim 14 (Currently Amended): The method of claim ~~[[11]]~~ 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 15 (Currently Amended): The method of claim ~~[[11]]~~ 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 16 (Currently Amended): A method for transferring data to a remoter internet server~~one or more remote internet servers~~ by a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled mobile device:

establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;

detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

 sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device[[.]] corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

 enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

 receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

 sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and time-stamp;

receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;

obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key;
and

sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server ~~to one or more remote internet servers.~~

Claim 17 (Currently Amended): The method of claim ~~[[15]]~~ 16, wherein the Bluetooth enabled mobile device configures the new data so that it can be received by ~~one or more remote internet servers~~ a remote internet server, and wherein configuring new data for receipt by ~~a remote internet server~~ one or more internet servers comprises specifying action setting and destination address of a remote internet server ~~one or more internet servers~~.

Claim 18 (Currently Amended): The method of claim ~~[[15]]~~ 16, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 19 (Currently Amended): The method of claim ~~[[15]]~~ 16, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 20 (Currently Amended): The method of claim ~~[[15]]~~ 16, wherein the time-stamp is either absolute time or relative time.

Remarks

Present Invention and Pending Claims

This invention relates generally to distribution of multimedia content. More particularly, this invention relates to pairing a data capture device in conjunction with a mobile device for automatically transferring data and multimedia content to one or more websites simultaneously.

Summary of the Office Action

Claims 1-20 are provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-20 of application no. 14295352. Although the conflicting claims are identical, they are not patentably distinct from each other because they are both similar.

Claims 1-20 are rejected under 35 AIA U.S.C. 103(a) as being unpatentable over Kennedy 20030157960 further in view of Vesuna US 20080272185.

Claim 3 is rejected under 35 U.S.C. AIA 103(a) as being unpatentable over Kennedy 20030157960 further in view of Vesuna US 20080272185 and further in view of Hong 20060264176.

Claims 1-2, 4-20 are rejected under 35 AIA U.S.C. 103(a) as being unpatentable over Kennedy 20030157960 further in view of Behzad US 20090023428.

Claim 3 is rejected under 35 U.S.C. AIA 103(a) as being unpatentable over Kennedy 20030157960 further in view of Behzad US 20090023428 and further in view of Hong 20060264176.

Amendment to the Claims

Claims 1, 6, 10 and 12-20 are currently amended.

The office action states: **“The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.”**

Applicant submits that, even though the present application was filed on or after March 16, 2013, the instant application is a continuation application and has an effective filing date of Dec 11, 2008. Therefore, the instant application must be examined under the first-to-invent provisions of pre-AIA law.

Examination Guidelines for Implementing the First Inventor To File Provisions of the Leahy-Smith America Invents Act, 78 Fed. Reg. 11059, 11083-84 (Feb. 14, 2013) states that: *“The AIA provides that the provisions of pre-AIA 35 U.S.C. 102(g) apply to each claim of an application for patent if the patent application: (1) Contains or contained at any time a claim to a claimed invention having an effective filing date that occurs before March 16, 2013; or (2) is ever designated as a continuation, divisional, or continuation-in-part of an application that contains or contained at any time a claim to a claimed invention that has an effective filing date before March 16, 2013.”*

For the reasons stated above, applicant submits that the above application must be examined under the first-to-invent provisions of pre-AIA law.

The office action states: **“Claims 1-20 are provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-20 of Application No. 14295352. Although the conflicting claims are identical, they are not patentably distinct from each other because they are both similar. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground**”

In response, a terminal disclaimer is filed herewith to overcome the non-statutory double patenting rejection of claims in the instant application over the claims 1-20 of application no. 14/295,352. Accordingly, applicant respectfully requests the above rejection be withdrawn.

The office action further states: **“Claims 1-20 are rejected under 35 AIA U.S.C. 103(a) as being unpatentable over Kennedy 20030157960 further in view of Vesuna US 20080272185.” AND**
“Claims 1-2, 4-20 are rejected under 35 AIA U.S.C. 103(a) as being unpatentable over Kennedy 20030157960 further in view of Behzad US 20090023428.”

In response, applicant submits that Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest all the limitations in the original claims 1, 6, 12 and 16.

Argument 1:

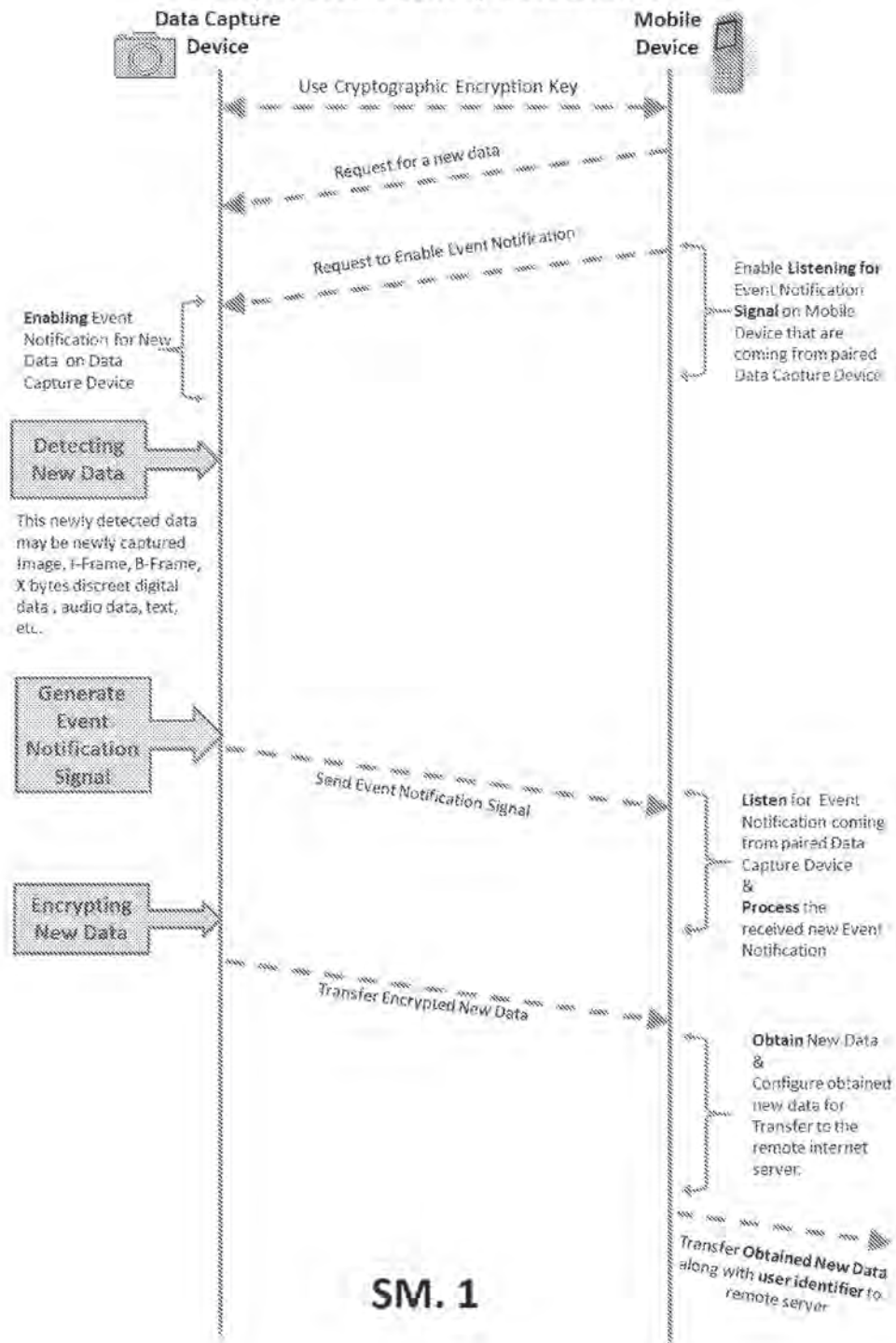
Claims 1 and 12 recite a method of transferring data to a remote internet server by a Bluetooth enabled mobile device.

Claim 1 recites the sequence of steps being performed at the Bluetooth enabled data capture device.

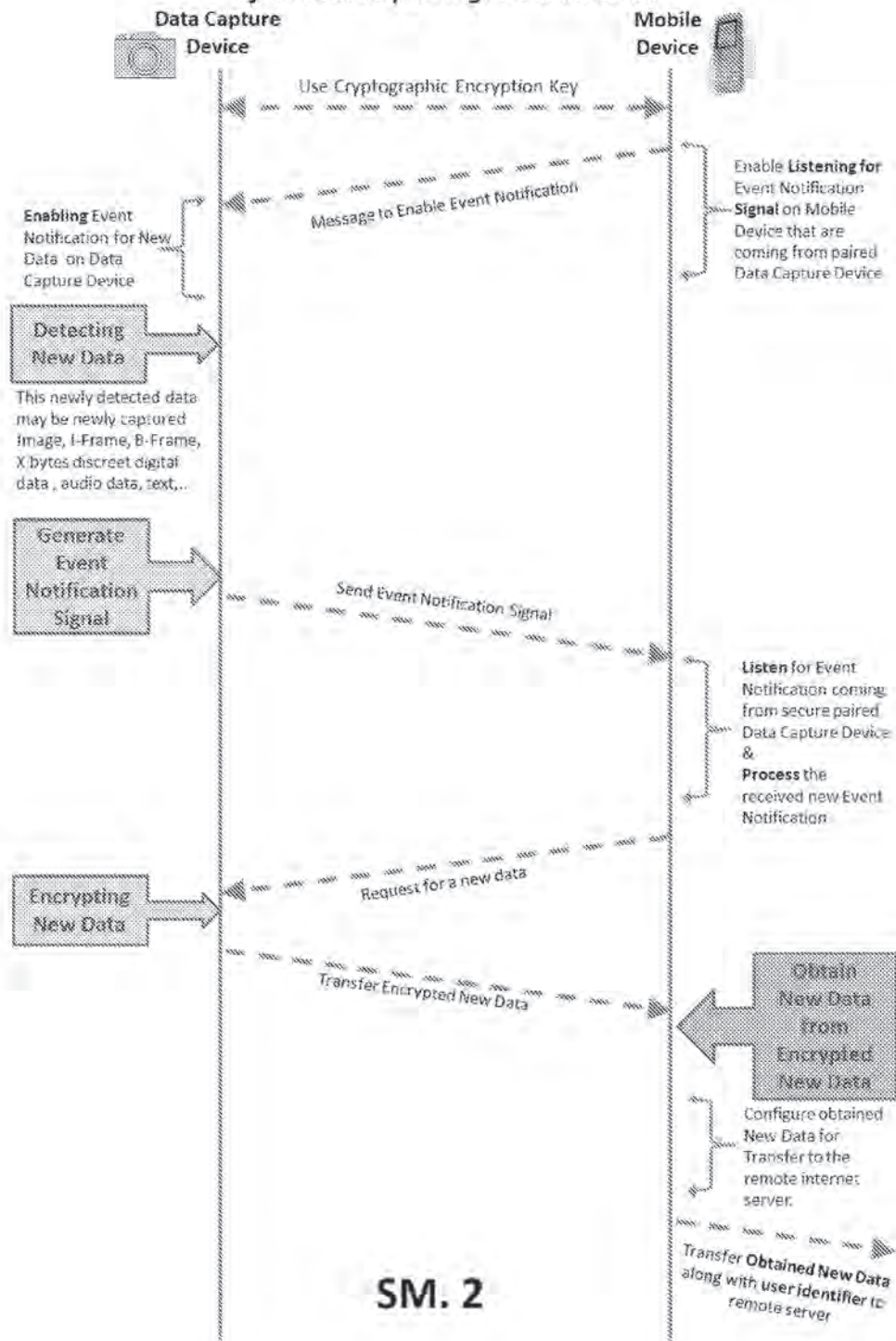
Claim 12 recites the sequence of steps being performed at the Bluetooth enabled mobile device.

The sequence of steps recited in claim 1 and the sequence of steps recited in claim 12 are illustrated in the **State Machine diagram, SM. 1 and State Machine diagram, SM. 2, shown below:**

State Machine Claim # 1
after secure pairing is established



State Machine Claim # 12
after secure pairing is established



SM. 2

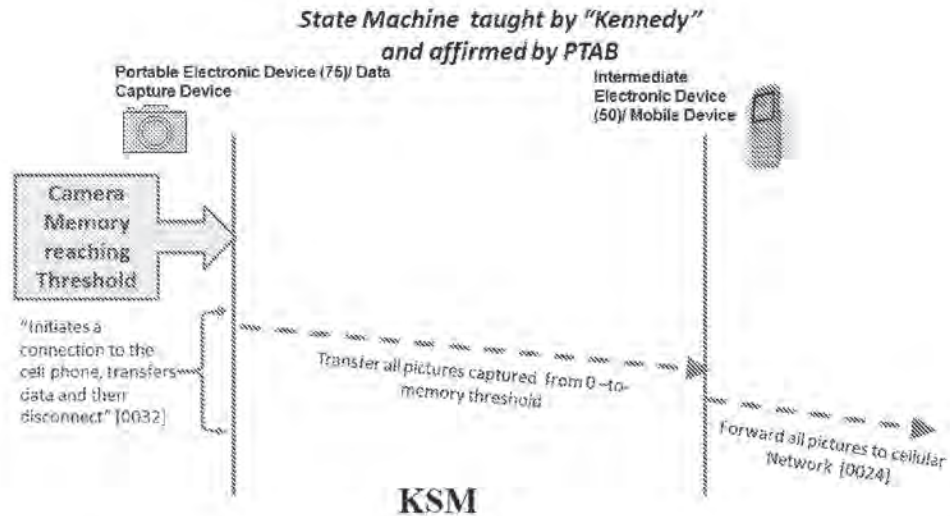
Claim 12 recites a series of steps performed at the mobile device for **detecting new data acquired in the Bluetooth enabled data capture device** for transfer. The first step comprises: **sending a message to the Bluetooth enabled data capture device over a previously established paired Bluetooth connection**. The message notifies the **Bluetooth enable data capture device to enable event notifications when new data is available for transfer from the Bluetooth enabled data capture device**.

Claim 1 which claims the sequence of steps performed at the Bluetooth enabled data capture device, recites a step corresponding to the above step in claim 12. Consequently, the **Bluetooth enabled data capture device receives a request**, for example, in the form of a message, **from the Bluetooth enabled mobile device**, where the **request requests the Bluetooth enabled data capture device to enable event notifications**, corresponding to **availability of new data for transfer**, on the Bluetooth enabled data capture device.

Kennedy **does not disclose that his intermediate electronic device 50 sends a request to his portable electronic device 75 to enable event notifications** which notify the availability of new data in the portable electronic device 75 for transfer.

In contrast, Kennedy discloses, *inter alia*, three modes: real-time, automatic, or manual mode to dynamically transfer data from the portable electronic device 75 to a remote storage device 25 through the intermediate electronic device 50 (see Kennedy, paragraphs [0030]-[0033]). As clearly illustrated in the **state-machine diagram** titled **KSM** below, Kennedy's portable electronic device 75 transfers the data:

- a) In real-time mode: immediately after the data is captured;
- b) In automatic mode: after its memory is full or nearly-full based upon a threshold value; and
- c) In manual mode: where a user of the portable electronic device 75 decides when to perform the transfer.



Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the following limitations in claims 1 and 12:

“receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection” *in claim 1*; and

“sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data” *in claim 12*.

As clearly illustrated by the **state-machine diagrams** titled **KSM, SM1 & SM2**, the state machines SM1 & SM2 are very different from state machine KSM.

Argument 2:

In the second step of claim 12, the Bluetooth enabled mobile device *enables event notification listening to listen for event notifications that are expected from the*

Bluetooth enabled data capture device when new data is available for transfer. **Claim 1 recites the corresponding** step comprising enabling event notification on Bluetooth enabled data capture device, *corresponding to new data*. The new data represents the immediately available new data in the Bluetooth enabled data capture compared to the previously transferred new data, if any, after the secure Bluetooth pairing connection is established.

Furthermore, **Kennedy does not disclose** the steps of **enabling event notifications** on the portable electronic device 75, corresponding to new data. Consequently, **Kennedy does not disclose** the step of **enabling event notification listening** on the intermediate electronic device 50. As explained above, Kennedy discloses sending the data acquired in the portable electronic device 75 to the intermediate electronic device 50, as quickly as the network connections allow, without determining if the intermediate electronic device 50 is ready to receive the acquired data.

Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad does not teach or suggest the following limitations:

“enabling event notification on Bluetooth enabled data capture device, corresponding to new data” *in claim 1*; and

“enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection” *in claim 12*.

Argument 3:

Claim 1 recites a third step of **determining existence of new data for transfer** to the Bluetooth enabled mobile device (see page 3, lines 16-21 of applicant’s original application). “**New data**” in the applicant’s case is data **acquired** in the Bluetooth enabled data capture device **after a paired Bluetooth connection is established** with the Bluetooth enabled mobile device. In the fourth step of claim 1, an event notification is

sent to the Bluetooth enabled mobile device, corresponding to the existence of new data for transfer. Consequently, the third step in claim 12 comprises: the Bluetooth enabled **mobile device receiving the event notification**, corresponding to existence of new data for transfer, from the Bluetooth enabled data capture device. As explained above, the Bluetooth enabled mobile device was continuously listening for the event notification from the Bluetooth enabled data capture device over the pre-established paired Bluetooth connection (see page 7, lines 26-31 of applicant's original application).

Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the above limitations. *Pages 5 and 8 of the office action suggest that Kennedy discloses the above limitations in paragraph [0010]. Applicant respectfully disagrees.* Kennedy discloses that data transfer occurs in one of three modes, namely, real-time, automatic, or manual (see Kennedy, paragraphs [0010] and [0030]-[0035]). However, **none of these modes involve: (a) determining the existence of new data** in the Bluetooth enabled data capture device for transfer, **(b) sending an event notification** to the Bluetooth enabled mobile device, corresponding to the existence of new data for transfer, where the Bluetooth enabled mobile device is listening for the event notification.

In applicant's disclosure, "new data" (in one case detected using a data and file monitoring and detection module 203b) may be a "new file" or a "new data object" captured by the camera, microphone, etc., after a paired Bluetooth connection is established. The Bluetooth enabled data capture device may have to determine "new data for transfer" for different data types and for different scenarios using different techniques (see page 6, lines 27-31 of applicant's original disclosure).

For example:

A. In case of video: Bluetooth enabled data capture may have to determine existence of New I-Frame or B-Frame multimedia object or the whole new video file in different file formats.

B. In case of text: Bluetooth enabled data capture may have to determine existence of new short text message or new text file.

C. In case of audio: Bluetooth enabled data capture may have to determine existence of new data object for AAC audio codec or other voice formats, or the whole new audio file in different audio formats.

D. In case of images: Bluetooth enabled data capture may have to determine existence of new image file, in some cases before image processing, i.e., sending raw image data file, or in some cases after image processing and compression i.e., after the image is compressed into JPEG format or PNG format or some other compression, or filter, depending upon the scenario.

E. In case of other digital data types: Bluetooth enabled data capture device may have to determine the existence of “new digital data” that may be 5 bytes or 20 bytes or 400 bytes and then start the signaling.

Points A-E are not required or taught in “Kennedy” mainly because **Kennedy’s disclosure depends on:**

“reaching memory threshold” and not on detection of any type of newly captured or acquired data/data object/file by for example, a data and file monitoring and detection module 203b, as disclosed by the applicant. Kennedy waits for size of captured data to reach a memory threshold set by the user, and then initiates connection with a mobile device (see Kennedy paragraph [0010]) and that could happen as an example, after 5 photos or 20 photos are captured on the data capture device.

Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad does not teach or suggest the following limitations:

“determining existence of the new data for transfer”; and

*“sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device” ***in claim 1;*** and*

“receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection” *in claim 12*.

Argument 4:

Amended claims 1 and 12 recite additional steps comprising: “using cryptographic encryption key” on a Bluetooth paired secured connection, which is a Personal Area Network (PAN), for communication between data capture device and mobile device. Other steps comprise “encrypting the new data acquired in the Bluetooth enabled data capture device using cryptographic encryption key, receiving encrypted data corresponding to the new data by the Bluetooth enabled mobile device, over the established Bluetooth paired secure wireless connection, and obtaining new data from the encrypted data using cryptographic encryption key”.

Kennedy further in view of Vesuna and Kennedy further in view of Behzad does not teach or suggest these new limitations. Behzad discloses encrypting the communication links i.e., the communication channels 140a to 140d for secured communication among the local host devices WMCD 130, 130c, 130d and the remote host or storage 150 (see Behzad, paragraph [0041] and FIG. 1). This is not the same as applicant’s limitation of receiving encrypted data from the Bluetooth enabled data capture device.

Behzad teaches encryption over the Internet connection (WAN) and NOT encryption over the Bluetooth connection (PAN) between data capture device and mobile device.

Behzad does *not* teach “obtaining new data from the received encrypted data on the Mobile device”. In Behzad’s case, obtaining data from the encrypted data would be done on the remote host/storage (see Behzad, paragraph [0041] and FIG. 1).

Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad **does not teach or suggest the following limitations:**

“receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key” *in claim 12.*

“transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, ,..., wherein the Bluetooth enabled mobile device is configured to receive the encrypted data, obtain the new data from the encrypted data using cryptographic encryption key,....” *in claim 1.*

“wherein the paired secure Bluetooth connection uses cryptographic encryption key” *in claim 1 and claim 12.*

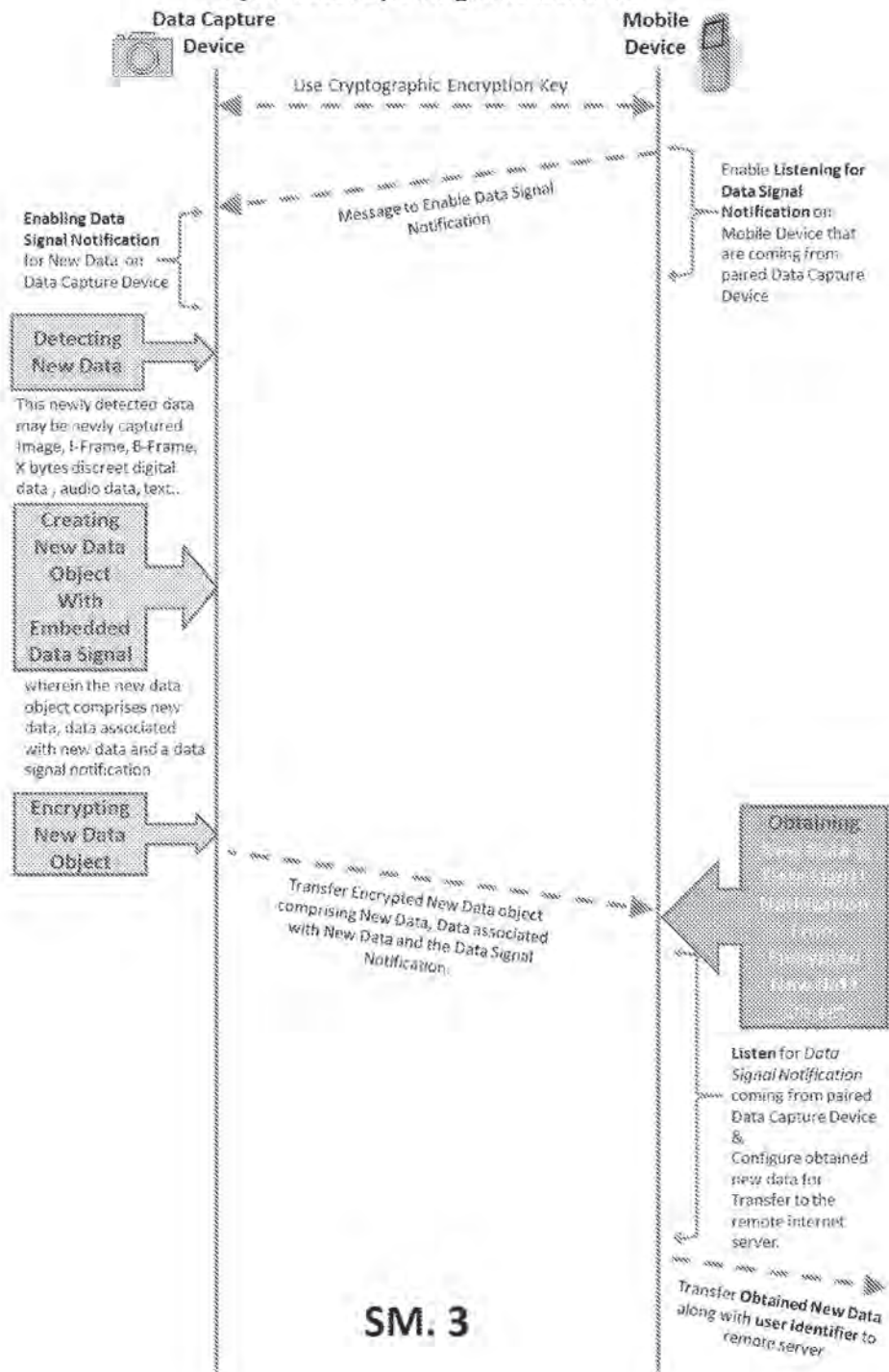
For the reasons stated above, applicant submits that even if Kennedy and Vesuna or Kennedy and Behzad are combined as suggested in the office action, there is no reasonable expectation of success in arriving at the above identified limitations in claims 1 and 12. Accordingly, applicant submits that claims 1 and 12 are non-obvious over the combination of Kennedy further in view of Vesuna, and also over the combination of Kennedy further in view of Behzad.

Argument 5:

Claim 6 also recites a method of transferring data to a remote internet server by a Bluetooth enabled mobile device,

Claim 6 recites the sequence of steps being performed at the Bluetooth enabled data capture device. **State Machine diagram, SM. 3, shown below, illustrates the sequence of steps recited in claim 6:**

State Machine Claim # 6
after secure pairing is established



Claim 6 recites that the Bluetooth enabled data capture device *receives a message* from the Bluetooth enabled mobile device to *register for data signal notifications so that the Bluetooth enabled data capture device may send event notifications whenever there is new data available for transfer* (see page 7, lines 21-31 of the applicant's application).

The office action suggests that these limitations are taught by Kennedy but does not identify the particular section in Kennedy where these limitations are found. The office action suggests that applicant's claim 6 corresponds to claim 1 and therefore the sections of Kennedy cited for claim 1 also apply for claim 6. Applicant respectfully disagrees. Moreover, **a review of Kennedy shows that Kennedy does not disclose the above limitations.** Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the following limitations in claim 6:

"receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device",

Claim 6 further recites the following limitation which is also found in claim 1:

"determining existence of the new data for transfer".

As shown for claim 1 in Argument # 3, Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the above limitation.

As clearly illustrated by the **state-machine diagrams, applicant's state machine SM3 is very different from Kennedy's state machine KSM.**

Argument 6:

Claim 6 also recites the step of *creating a new data object comprising new data, data associated with new data and a data signal notification*. As explained above, in the applicant's case, "new data object" may be a new video object, a new text message or file, a new audio object, an image object, etc. Data associated with the new data may comprise:

A. In case of video object: length of the video, video codec used for creating the video, time, etc.

B. In case of text message or file object: Formatting associated with the text message or file, number of characters in the text message or file, time, etc.

C. In case of audio object: length of the audio, audio codec used for creating the video, time, etc.

D. In case of image object: size of the image, image format, time, etc.

E. In case of other digital data object types: Size of the data object, time, and other metadata associated with the object.

Kennedy does not disclose the step of creating a new data object using new data which is acquired after a paired Bluetooth connection is established between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device.

Kennedy also does not disclose that the new data object comprises new data, data associated with new data and a data signal notification which is a time-stamp attribute.

More specifically, the data signal notification corresponds to existence of new data for transfer. Kennedy does not disclose anything similar to the applicant's data signal notification. Accordingly, Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the following limitation:

"creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer" *in claim 6*

Argument 7:

Next, **claim 6** recites the step of encrypting the new data in the Bluetooth enabled data capture device, using a cryptographic encryption key.

Kennedy, Vesuna and Hong do not disclose encrypting data. Behzad discloses encrypting the communication links i.e., the communication channels 140a to 140d for secured communication among the local host devices WMCD 130, 130c, 130d and the remote host or storage 150 (see Behzad, paragraph [0041] and FIG. 1). Therefore, Behzad also does not disclose the applicant's limitation of encrypting the new data in the Bluetooth enabled data capture device, using a cryptographic encryption key.

Behzad teaches encryption over the Internet connection (WAN) and NOT encryption over the Bluetooth connection(PAN) between data capture device and mobile device.

Accordingly, Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the following limitations:

"encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device" *in claim 6; and*

"transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection" *in claim 6.*

For the reasons stated above, applicant submits that even if Kennedy and Vesuna or Kennedy and Behzad are combined as suggested in the office action, there is no reasonable expectation of success in arriving at the above identified limitations in claim 6. Accordingly, applicant submits that claim 6 are non-obvious over the combination of Kennedy further in view of Vesuna, and also over the combination of Kennedy further in view of Behzad.

Argument 8:

Claim 16 recites the following steps which are also recited in claim 12:

“sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device, corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device”;

“enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection”;

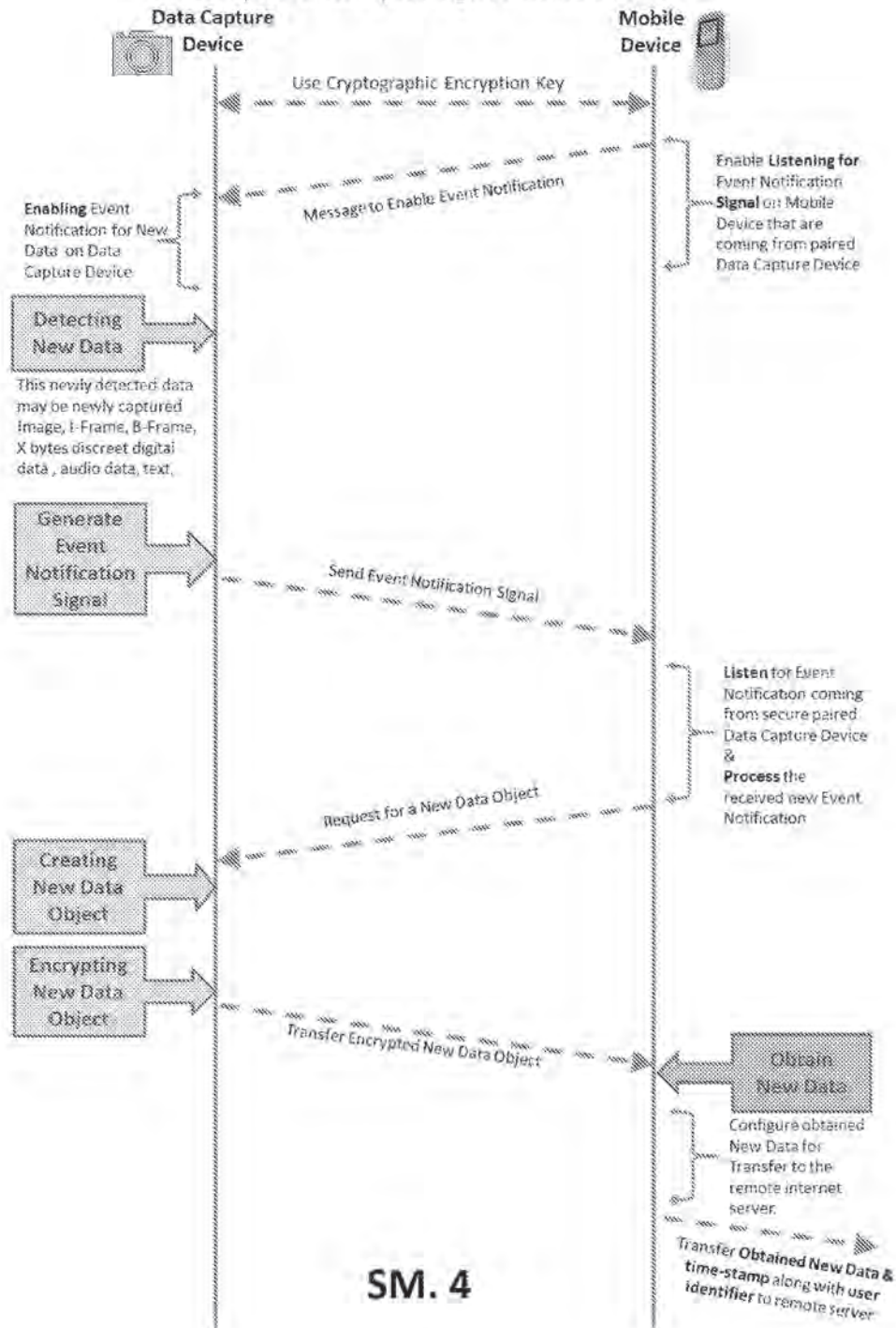
“receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection”;

“receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection” and

“obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key”.

The state machine diagram, SM 3, shown below illustrates the sequence of steps performed in claim 16.

State Machine Claim # 16
after secure pairing is established



As shown for claim 12 in Argument #1 and Argument #2, Kennedy further in view of Vesuna and Kennedy further in view of Behzad does not teach or suggest the above limitations.

As clearly illustrated by the state-machine diagrams, applicant's state machine SM4 is very different from Kennedy's state machine KSM.

Argument 9:

Claim 16 also recites that the Bluetooth enabled mobile device *sends a request* to the Bluetooth enabled data capture device *to get new data object for transfer*. This step is *performed immediately after* the Bluetooth enabled mobile device *receives an event notification, corresponding to existence of new data for transfer*, from the Bluetooth enabled data capture device.

In Kennedy, no such request is sent from the intermediate electronic device 50 to the portable electronic device 75. Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest the following limitations:

“sending a request to the Bluetooth enabled data capture device, to get new data object for transfer” *in claim 16*.

Argument 10:

Amended claim 16 recites additional steps comprising “using cryptographic encryption key” on the PAN network for communication between data capture device and mobile device. Other steps comprise: “receiving encrypted data corresponding to the new data by the Bluetooth enabled mobile device, over the established Bluetooth paired secure wireless connection, and obtaining new data from the encrypted data using cryptographic encryption key”.

Kennedy further in view of Vesuna and Kennedy further in view of Behzad do not teach or suggest these new limitations. Behzad discloses encrypting the communication links i.e., the communication channels 140a to 140d for secured communication among the local host devices WMCD 130, 130c, 130d and the remote host or storage 150 (see Behzad, paragraph [0041] and FIG. 1). This is not the same as applicant's limitation of receiving encrypted data from the Bluetooth enabled data capture device.

Behzad teaches encryption over the Internet connection (WAN) and NOT encryption over the Bluetooth connection (PAN) between data capture device and mobile device.

Behzad does *not* teach "obtaining new data, data associated with new data and time-stamp from the received encrypted data object on the Mobile device using cryptographic encryption key". In Behzad's case obtaining data from the encrypted data would be done on the remote host/storage. (see Behzad, paragraph [0041] and FIG. 1).

Therefore, Kennedy further in view of Vesuna and Kennedy further in view of Behzad **does not teach or suggest the following limitations:**

"wherein the paired secure Bluetooth connection uses cryptographic encryption key" in claim 16;

"receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection" in claim 16;

"obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key" in claim 16;
and

“sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server” in claim 16.

For the reasons presented above, applicant submits that even if Kennedy and Vesuna or Kennedy and Behzad are combined as suggested in the office action, there is no reasonable expectation of success in arriving at the limitations recited in applicant's claim 16. Therefore, applicant respectfully requests the rejection of claim 16 be reconsidered and withdrawn.

Claims 2-5, 7-11, 13-15 and 17-20 are dependent on claims 1, 6, 12 and 16 respectively. Since claims 1, 6, 12 and 16 are non-obvious over Kennedy further in view of Vesuna, applicant submits that dependent claims 2-5, 7-11, 13-15 and 17-20 are also non-obvious over Kennedy further in view of Vesuna. *Therefore, applicant respectfully requests the rejection of above dependent claims be withdrawn.*

Claims 2, 4, 5 are dependent on claim 1; claims 7-11, 13-15 and 17-20 are dependent on claims 6, 12 and 16 respectively. Since claims 1, 6, 12 and 16 are non-obvious over Kennedy further in view of Behzad, applicant submits that dependent claims 2, 4, 5, 7-11, 13-15 and 17-20 are also non-obvious over Kennedy further in view of Behzad. *Therefore, applicant respectfully requests the rejection of above dependent claims be withdrawn.*

The office action further states: **“Claim 3 is rejected under 35 U.S.C. AIA 103(a) as being unpatentable over Kennedy 20030157960 further in view of Vesuna US 20080272185 and further in view of Hong 20060264176.” AND**

“Claim 3 is rejected under 35 U.S.C. AIA 103(a) as being unpatentable over Kennedy 20030157960 further in view of Behzad US 20090023428 and further in view of Hong 20060264176.”

Claim 3 is dependent on claim 1. Kennedy further in view of Vesuna and further in view of Hong or Kennedy further in view of Behzad and further in view of Hong do

not teach or suggest all the limitations in claim 1. Therefore, claim 1 is non-obvious over the combination of Kennedy further in view of Vesuna and further in view of Hong; and also non-obvious over the combination of Kennedy further in view of Behzad and further in view of Hong. Therefore, applicant submits that dependent claim 3 is also non-obvious over the combination of Kennedy further in view of Vesuna and further in view of Hong; and also non-obvious over the combination of Kennedy further in view of Behzad and further in view of Hong.

Accordingly, applicant respectfully requests the rejection of claim 3 be reconsidered and withdrawn.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. In the interest of compact prosecution, if the prosecution of the application can be advanced or if a claim may be made potentially allowable by an Examiner's amendment, applicant requests Examiner Nooristany to call the undersigned with the proposed amendment.

Respectfully submitted,

Date: Aug 05, 2014

/a tankha/
Ashok Tankha
Attorney for Applicant
Reg. No. 33,802

Correspondence Address

Lipton, Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Fax: 856-374-0246
Phone: 856-266-5145
Email: ash@ipprocure.com

TERMINAL DISCLAIMER TO OBTAIN A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) CellSpin_04Con7_US
In re Application of: Gurvinder Singh, Marcos Klein and Vince Laviano Application No.: 14/295,353 Filed: 06/04/2014 For: Automatic Multimedia Upload For Publishing Data And Multimedia Content The owner*, CellSpinsoft Inc., of <u>100</u> percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number <u>14295352</u>, filed <u>04 June 2014</u>, as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns. In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that: any such patent: granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant. Check either box 1 or 2 below, if appropriate. 1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon. 2. ☒ The undersigned is an attorney or agent of record. Reg. No. <u>33802</u> <u>/s tankha/</u> Signature 08-05-2014 Date <u>Ashok Tankha</u> Typed or printed name 856-266-5145 Telephone Number ☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included. WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. *Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this statement. See MPEP § 324.	

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Application Number 	Application/Control No.	Applicant(s)/Patent under Reexamination	
	14/295,353	SINGH ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☐ APPROVED	☒ DISAPPROVED
Date Filed : 8/5/14	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
Janice Ford Resubmit terminal along with a 3.73(c) statement.

U.S. Patent and Trademark Office



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/295,353	06/04/2014	Gurvinder Singh	CellSpin_04Con7_US	9544
Ashok Tankha 36 Greenleigh drive Sewell, NJ 08080			EXAMINER NOORISTANY, SULAIMAN	
			ART UNIT 2478	PAPER NUMBER
			MAIL DATE 07/08/2014	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 14/295,353	Applicant(s) SINGH ET AL.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2478	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 6/4/14.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☒ Claim(s) 1-20 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☒ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) ____ is/are objected to.

9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some** c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date ____.

4) ☐ Other: ____.

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Detailed Action

This Office Action is response to the application (14295353) filed on 6/4/14

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-20 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-20 of Application No. 14295352. Although the conflicting claims are identical, they are not patentably distinct from each other because they are both similar.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

The following is a quotation of AIA 35 U.S.C. 103(a), which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-20 are rejected under 35 AIA U.S.C. 103(a) as being unpatentable over Kennedy 20030157960 further in view of Vesuna US 20080272185.

1. Kennedy teaches a method for transferring data from a Bluetooth enabled data capture device to one or more remote internet servers via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device (fig. 1, unit 75 & unit 50);

establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device (fig. 1, unit 75 & unit 50 [0009]);

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired Bluetooth connection is established [0010];

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer [0010] comprises:

receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection [0010];

receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection [0010];

enabling event notification on Bluetooth enabled data capture device, corresponding to change in new data [0010];

determining existence of the new data for transfer [0010]; and

sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device [0010, 0023-0024];

transferring the new data acquired in the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the new data and send data and [[timestamp]] to one or more remote internet servers ([0010, 0023-0024], fig. 1, unit 25).

Kennedy merely discloses the term 'timestamp'

Vesuna teaches that it is well known to have system to include timestamp to servers ([0030]) in order to attach a time-stamp to the scanned or read information so that the time of the transaction is accurately recorded [0030].

Thus, it would have been obvious to one ordinary skill in the art before the effective filing date of the invention to modify Kennedy's invention in order to identify captured event or stored data for future retrieval [0030], as taught by Venuna.

2. The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device (fig. 2, unit 170).

4. The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data (Kennedy: [0010]).

5. The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer (Kennedy: [0010]).

Claim 3 is rejected under 35 U.S.C. AIA 103(a) as being unpatentable over Kennedy 20030157960 further in view of Vesuna US 20080272185 and further in view of Hong 20060264176.

Claim 3: Kennedy merely discloses wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Hong teaches that it is well known to have system wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module (e.g., Fig. 1 - [0024-0025]) in order to make the system more efficient by utilizing mobile phones to receive the data without any internal wireless Bluetooth interface through Bluetooth transmitter wirelessly [0025].

Thus, it would have been obvious in one ordinary skill in the art before the effective filing date of the invention to modify Kennedy's invention by utilizing mobile phones to receive the electronic product without any internal wireless Bluetooth interface through Bluetooth transmitter wirelessly [0025], as taught by Hong.

Claim 6-20 are rejected for similar reason as stated above.

Claims 1-2, 4-20 are rejected under 35 AIA U.S.C. 103(a) as being unpatentable over Kennedy 20030157960 further in view of Behzad US 20090023428.

1. Kennedy teaches a method for transferring data from a Bluetooth enabled data capture device to one or more remote internet servers via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device (fig. 1, unit 75 & unit 50);

establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device (fig. 1, unit 75 & unit 50 [0009]);

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired Bluetooth connection is established [0010];

detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer [0010] comprises:

receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection [0010];

receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection [0010];

enabling event notification on Bluetooth enabled data capture device, corresponding to change in new data [0010];

determining existence of the new data for transfer [0010]; and
sending event notification as a signal to the Bluetooth enabled mobile device,
corresponding to existence of new data for transfer, over the established paired
Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event
notification sent from the Bluetooth enabled data capture device [0010, 0023-0024];
transferring the new data acquired in the Bluetooth enabled data capture to the
Bluetooth enabled mobile device, over the paired Bluetooth connection, wherein the
Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth
enabled mobile device is configured to receive the new data and send data and
[[timestamp]] to one or more remote internet servers ([0010, 0023-0024], fig. 1, unit 25).

Kennedy merely discloses the term 'timestamp'
Behzad teaches that it is well known to have system to include timestamp to servers (fig
1, unit 141 "time, date") in order to identify captured event or stored data for future
retrieval [0030].

Thus, it would have been obvious to one ordinary skill in the art before the
effective filing date of the invention to modify Kennedy's invention in order to identify
captured event or stored data for future retrieval [0030], as taught by Behzad.

2. The method of claim 1, wherein Bluetooth capability is provided internally in
the Bluetooth enabled data capture device (fig. 2, unit 170).

4. The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data (Kennedy: [0010]).

5. The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer (Kennedy: [0010]).

Claim 3 is rejected under 35 U.S.C. AIA 103(a) as being unpatentable over Kennedy 20030157960 further in view of Behzad US 20090023428 and further in view of Hong 20060264176.

Claim 3: Kennedy merely discloses wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.

Hong teaches that it is well known to have system wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module (e.g., Fig. 1 - [0024-0025]) in order to make the system more efficient by utilizing mobile phones to receive the data without any Internal wireless Bluetooth interface through Bluetooth transmitter wirelessly [0025].

Thus, it would have been obvious in one ordinary skill in the art before the effective filing date of the invention to modify Kennedy's invention by utilizing mobile phones to receive the electronic product without any internal wireless Bluetooth interface through Bluetooth transmitter wirelessly [0025], as taught by Hong.

Claim 6-20 are rejected for similar reason as stated above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is (571) 270-1929. The examiner can normally be reached on M-F from 9 to 5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Derrick Ferris, can be reached on (571) 272-3123. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Sulaiman Nooristany/

Primary Examiner, Art Unit 2478

AUTOMATIC MULTIMEDIA UPLOAD FOR PUBLISHING DATA AND MULTIMEDIA CONTENT

CROSS REFERENCE TO RELATED APPLICATIONS

5

1. This application is a continuation application of non-provisional patent application
number 14/172,913, titled "Automatic multimedia upload for publishing multimedia
content", filed on February 05, 2014 in the United States Patent and Trademark
Office, which is a continuation application of non-provisional patent application
10 number 13/740,214, titled "Automatic multimedia upload for publishing multimedia
content", filed on January 13, 2013 in the United States Patent and Trademark Office,
which is a continuation application of non-provisional patent application number
12/333,303, now Patent no. 8392591, titled "Automatic multimedia upload for
publishing multimedia content", filed on December 11, 2008 in the United States
15 Patent and Trademark Office, which claims the benefit of US provisional patent
application number 61/017,202, titled "Automatic multimedia upload for publishing
multimedia content", filed on December 28, 2007 in the United States Patent and
Trademark Office. The specifications of the above referenced applications are
incorporated herein by reference in their entirety.
- 20 2. The following patent application is incorporated herein in its entirety: US Non-
provisional patent application serial number 11/901,802, titled "Online Publishing Of
Multimedia Content", filed on September 19, 2007 in the United States Patent and
Trademark Office.

25

BACKGROUND

This invention, in general, relates to distribution of multimedia content. More
particularly, this invention relates to pairing a digital data capture device in conjunction
30 with a mobile device for automatically publishing data and multimedia content on one or
more websites simultaneously.

A user may need to capture and publish data and multimedia content on the internet in real time. Typically, the user would capture an image using a digital camera or a video camera, store the image on a memory device of the digital camera, and transfer
5 the image to a computing device such as a personal computer (PC). In order to transfer the image to the PC, the user would transfer the image off-line to the PC, use a cable such as a universal serial bus (USB) or a memory stick and plug the cable into the PC. The user would then manually upload the image onto a website which takes time and may be inconvenient for the user.

10

Therefore, there is a need for a method and system to utilize a digital data capture device in conjunction with a mobile device for automatically detecting capture of data and multimedia content, transferring the captured data and multimedia content to the mobile device, and publishing the data and multimedia content on one or more websites
15 automatically or with minimal user intervention.

SUMMARY OF THE INVENTION

This summary is provided to introduce a selection of concepts in a simplified
20 form that are further described in the detailed description of the invention. This summary is not intended to identify key or essential inventive concepts of the claimed subject matter, nor is it intended for determining the scope of the claimed subject matter.

The method and system disclosed herein addresses the above stated need for
25 utilizing a digital data capture device in conjunction with a Bluetooth™ (BT) enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. The digital data capture device is physically separated from the BT enabled mobile device.

30 In the method and system disclosed herein, a client application is provided on a BT enabled mobile device. In the absence of in-built BT capability in the digital data

capture device, a BT communication device is provided on the digital data capture device. The BT communication device may, for example, be an in-built BT capability chip, a BT memory card, or an external BT device. The BT communication device on the digital data capture device is paired with the BT enabled mobile device to establish a
5 connection between the digital data capture device and the BT enabled mobile device.

A user may capture data and multimedia content using the digital data capture device. The digital data capture device may, for example, be a digital camera, a video camera, or other digital modular camera systems. The client application on the BT
10 enabled mobile device detects the captured data, multimedia content, and files associated with the captured data and the multimedia content on the digital data capture device by communicating over a wireless BT protocol. The captured data, multimedia content, and the associated files are automatically transferred to the client application on the BT
enabled mobile device from the digital data capture device.

15 The detection and transfer of the captured data, the multimedia content, and the associated files may be initiated by the client application of the BT enabled mobile device. The detection and transfer of the captured data, the multimedia content, and the associated files to the BT enabled mobile device may be initiated by the digital data
20 capture device when the client application is unable to detect the captured data, the multimedia content, and the associated files from the digital data capture device.

The user may configure a timer setting and select the websites for publishing using the client application on the BT enabled mobile device. The client application
25 selects the websites for publishing the transferred data and the multimedia content based on user preferences configured on the Bluetooth enabled mobile device. The client application also sets time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The client application on the BT enabled
mobile device automatically publishes the transferred data and multimedia content on one
30 or more websites using the settings configured by the user. The method and system disclosed herein thereby enables the user to capture data and multimedia content, for

example, audio, video, text, and images, automatically upload the captured data and multimedia content onto a BT enabled mobile device, and publish the data and multimedia content on one or websites automatically or with minimal user intervention. The user may therefore publish data and the multimedia content on immediate capture of
5 the data and the multimedia content on the digital data capture device.

The method and system disclosed herein is described with reference to a BT communication protocol. The method and system disclosed herein may be realized with wireless protocols, for example, Zigbee[®] protocol, Wibree[™] protocol, Ultra-Wide Band
10 (UWB) protocol, and other wireless protocols for wireless personal area networks.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing summary, as well as the following detailed description of the
15 invention, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, exemplary constructions of the invention are shown in the drawings. However, the invention is not limited to the specific methods and instrumentalities disclosed herein.

20 FIG. 1 illustrates a method of utilizing a digital data capture device in conjunction with a Bluetooth enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention.

FIG. 2 illustrates a system for utilizing a digital data capture device in conjunction with a
25 Bluetooth enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention.

FIGS. 3A-3C exemplarily illustrate the Bluetooth communication device options used on the digital data capture device for establishing a Bluetooth connection with the client
30 application on the Bluetooth enabled mobile device.

FIG. 4 exemplarily illustrates a system for publishing data and the multimedia content using a client application on a mobile device on one or more websites simultaneously.

FIG. 5 exemplarily illustrates a user utilizing a digital camera in conjunction with a Bluetooth enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates a method of utilizing a digital data capture device **201** in conjunction with a Bluetooth™ enabled mobile device **202** for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. The term “Bluetooth enabled mobile device” is herein referred to as “mobile device”. The digital data capture device **201** is physically separated from the mobile device **202** as illustrated in FIG. 2. The digital data capture device **201** may, for example, be a digital camera, a video camera, digital modular camera systems, or other digital data capturing systems.

In the method disclosed herein, a client application **203** is provided **101** on the mobile device **202**. In the absence of inbuilt Bluetooth (BT) capability in the digital data capture device **201**, a BT communication device **201a** is provided **102** on the digital data capture device **201**. The BT communication device **201a** may, for example, be an inbuilt BT capability chip **301**, a BT memory card **302**, or an external BT device **303** as illustrated in FIGS. 3A-3C respectively. The external BT device **303** may, for example, be attached to a universal serial bus (USB), a firewire interface, or a power port of the digital data capture device **201**. BT provides a method of connecting and exchanging information between devices, for example, mobile phones, laptops, personal computers (PCs), printers, digital cameras, etc. over a secure and globally unlicensed short-range radio frequency.

The BT communication device **201a** on the digital data capture device **201** is paired **103** with the mobile device **202** to establish a connection between the digital data capture device **201** and the mobile device **202**. BT pairing involves establishing a connection between two BT devices that mutually agree to communicate with each other.

5 A BT device that wants to communicate only with a trusted device can cryptographically authenticate the identity of another BT device. BT pairing occurs when the BT communication device **201a** agrees to communicate with the mobile device **202** in order to establish a connection. In order to initiate the pairing process between the BT communication device **201a** and the mobile device **202**, a common password known as a

10 passkey is exchanged between the BT communication device **201a** and the mobile device **202**. A passkey is a code shared by the BT communication device **201a** and the mobile device **202**.

A user sets a discoverable mode for the mobile device **202**. When set to the

15 discoverable mode, the mobile device **202** will allow the BT communication device **201a** on the digital data capture device **201** to detect the mobile device's **202** presence and attempt to establish a connection. In order to initiate the pairing process, the BT communication device **201a** will send the BT communication device name of a predefined number of characters, for example, up to 255 characters, and the BT address

20 to the mobile device **202**. The BT communication device **201a** then prompts the user of the mobile device **202** to enter the passkey code in order to accept the pairing with the BT communication device **201a** on the digital data capture device **201**. On entering the passkey by the user of the mobile device **202**, the entered passkey is matched with the passkey of the BT communication device **201a**. If a match is found, a trusted pair is

25 automatically established.

The user captures **104** data and multimedia content using the digital data capture device **201**. The data and multimedia content may, for example, comprise image files, audio files, video files, text files, or any combination thereof. The client application **203**

30 on the mobile device **202** detects **105** the captured data, the multimedia content, and files associated with the captured data and the multimedia content. The client application **203**

then initiates the transfer of the captured data, the multimedia content, and the associated files in a pull mode of operation. In the pull mode, the client application **203** periodically polls the digital data capture device **201** to determine the creation of a new file in the digital data capture device **201**. The digital data capture device **201** then automatically
5 transfers **106** the captured data, the multimedia content, and the associated files to the client application **203** on the mobile device **202** using one or a combination of file transfer protocols. The file transfer protocols may, for example, be one or a combination of BT profile protocols such as the object exchange (OBEX) protocol, the generic object exchange profile (GOEP) protocol, etc. The file transfer protocols may, for example, also
10 be the media transfer protocol (MTP), the picture transfer protocol (PTP), and the PictBridge protocol implemented using a USB.

The picture transfer protocol (PTP) allows the transfer of images from digital cameras to computers and other peripheral devices without the need of additional device
15 drivers. The media transfer protocol is a custom extension to the PTP and allows the protocol to be used for devices other than digital cameras, for example digital audio players and other portable media devices, for example portable video players. The PictBridge protocol allows images to be printed directly from digital cameras to a printer, without having to connect the camera to a computer.

20 The transfer of the data, the multimedia content, and the associated files may also take place in a push mode of operation. In the push mode, the BT communication device **201a** sends a signal to the client application **203** on creation of a new file. By implementation of a handshake protocol, the BT communication device **201a**
25 automatically transfers captured data, the multimedia content, and the associated files to the client application **203** on the mobile device **202**. For some external digital data capture devices, the client application **203** may not be able to detect the creation of a new file. In such cases, the digital data capture device **201** signals the client application **203** in the event a new file is created. A file event listener in the client application **203** listens for
30 the signal from the digital data capture device **201**. The user may then initiate the transfer by a press of a button or a key on the digital data capture device **201**.

In the case of a mobile device **202** with limited memory and processing capabilities, the client application **203** partitions the multimedia content of large files stored on the mobile device **202** into multiple data segments. The data segments are
5 tagged with segment identifiers using the client application **203**. The tagged data segments are transferred from the client application **203** of the mobile device **202** to a publishing service **401** via a network **402** as illustrated in FIG. 4.

When the client application **203** is unable to detect the captured data, the
10 multimedia content, and the associated files from the digital data capture device **201**, the digital data capture device **201** initiates detection and transfer of the captured data, the multimedia content, and the associated files to the mobile device **202**.

The user may also set preferences on the mobile device **202**. The user preferences
15 may, for example, comprise the websites selected for publishing the data and the multimedia content. The user may configure a timer setting and the websites on the mobile device **202** for publishing the data and the multimedia content. The user may also set timer and action settings for publishing the data and the multimedia content. The user may set the timer setting to, for example, a “no-wait-automatic” setting, a “wait-X-
20 minutes-automatic” setting, and a “wait-X-minutes-user-input-cancel” setting. The client application **203** on the mobile device **202** selects the websites for publishing the transferred data and the multimedia content based on user preferences configured on the mobile device **202**. The client application **203** also sets time for publishing the transferred data and the multimedia content automatically or with minimal user intervention.

25 The client application **203** on the mobile device **202** then automatically publishes **107** the transferred data and multimedia content on one or more websites. If the user configures the timer setting to “no-wait-automatic”, the data and the multimedia content are automatically published on one or more websites based on the user preferences
30 configured on the mobile device **202** without waiting for a certain period of time. If the user configures the timer setting to “wait-X-minutes-automatic”, the client application

203 will wait for “X” minutes for the user to change or cancel publishing. If there is no user action for “X” minutes, the client application **203** will automatically publish the data and multimedia content to one or more websites based on the user preferences. Further, if the user configures the timer setting to “wait-X-minutes-user-input-cancel”, the client
5 application **203** will wait for “X” minutes for an input from the user. If there is no input from the user, the client application **203** cancels the publishing of the data and multimedia content. The publishing of the data and multimedia content on one or more websites simultaneously is explained in the detailed description of FIG. **4**.

10 The user may therefore capture data, for example, audio, video, text, and images, automatically upload the captured data onto the mobile device **202**, and publish the data and multimedia content on one or websites automatically or with minimal user intervention. The method disclosed herein thereby enables the user to publish data and the multimedia content on immediate click of an image or recording of a video on the
15 digital data capture device **201** without having to manually upload the data onto a computing device and then publish the data on the websites.

FIG. **2** illustrates a system for utilizing a digital data capture device **201** in conjunction with a BT enabled mobile device **202** for publishing data and multimedia
20 content on one or more websites automatically or with minimal user intervention. The system disclosed herein comprises a digital data capture device **201** and a client application **203** provided on the BT enabled mobile device **202**. The digital data capture device **201** and the mobile device **202** are physically separated from each other. The digital data capture device **201** comprises a BT communication device **201a** and a data
25 capture module **201d**.

The BT communication device options used on the digital data capture device **201** for establishing a BT connection with the client application **203** on the BT enabled mobile device **202** are exemplarily illustrated in FIGS. **3A-3C**. The BT communication
30 device **201a** may, for example, be an in-built BT capability chip **301** as illustrated in FIG.

3A, a BT memory card **302** as illustrated in FIG. **3B**, or an external BT device **303** as illustrated in FIG. **3C**.

The BT communication device **201a** comprises a BT association protocol module **201b** and a data transfer protocol module **201c**. The client application **203** on the mobile device **202** comprises a BT association protocol module **203a**, a data and file monitoring and detection module **203b**, a data transfer protocol module **203c**, a data storage module **203d**, a graphical user interface (GUI) **203e**, and a media publishing module **203f**. The BT association protocol module **201b** of the digital data capture device **201** and the BT association protocol module **203a** of the client application **203** enable the pairing between the BT communication device **201a** and the mobile device **202**. The pairing of the BT communication device **201a** and the mobile device **202** is explained in the detailed description of FIG. **1**. The data capture module **201d** captures the data and the multimedia content on the digital data capture device **201**.

The data and file monitoring and detection module **203b** of the client application **203** monitors and detects the capture of the data, the multimedia content, and the files associated with the captured data and the multimedia content. On detection, the data transfer protocol module **203c** of the client application **203** initiates the transfer and download of the captured data, the multimedia content, and the associated files from the digital data capture device **201**. When the client application **203** is unable to detect the captured data, the multimedia content, and the associated files from the digital data capture device **201**, the data transfer protocol module **201c** of the digital data capture device **201** initiates the transfer of the captured data, the multimedia content, and the associated files to the mobile device **202**.

The data transfer protocol module **201c** of the digital data capture device **201** transfers the captured data, the multimedia content, and the associated files to the client application **203**. The data storage module **203d** stores the captured data, the multimedia content, and the associated files on the mobile device **202**. The user may also set preferences on the mobile device **202** using the GUI **203e** of the client application **203**.

The user preferences may, for example, comprise the websites selected for publishing the data and the multimedia content. The GUI **203e** enables the user to configure a timer setting and websites on the mobile device **202** for publishing the data and the multimedia content. The user may also set timer and action settings for publishing the data and the multimedia content using the GUI **203e**. The user may set a timer setting, for example, a “no-wait-automatic” setting, a “wait-X-minutes-automatic” setting, and a “wait-X-minutes-user-input-cancel” setting as explained in the detailed description of FIG. **1**.

The media publishing module **203f** automatically publishes the transferred data and the multimedia content on one or more of the websites. The media publishing module **203f** comprises a website selection module **203g**, a timer module **203h**, a segmentation module **203i**, and a data transfer module **203j**. The website selection module **203g** selects the websites for publishing the data and the multimedia content based on settings and user preferences configured by the user on the mobile device **202**. The timer module **203h** sets the time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The timer setting may be set for automatic publishing of the multimedia content or a time based wait mode where user interaction is required. The timer module **203h** sets the timer based on a timer setting, for example, a “no-wait-automatic” setting, a “wait-X-minutes-automatic” setting, and a “wait-X-minutes-user-input-cancel” setting configured by the user. The timer module **203h** ensures that if the user does not wish to publish the transferred data and multimedia content, the user has time to decide whether to publish or not. The user may also configure the client application **203** to automatically delete the data, the multimedia content, and the associated files after the data and the multimedia content have been posted and published on one or more websites based on user preferences.

In the case of a mobile device **202** with limited memory and processing capabilities, the client application **203** partitions the multimedia content of large files stored on the mobile device **202** into multiple data segments using the segmentation module **203i**. The segmentation module **203i** generates segment identifiers and tags the data segments with the segment identifiers. The data transfer module **203j** transfers the

data, the tagged data segments, and the multimedia content from the client application **203** to the publishing service **401** via a network **402** for publishing on the websites automatically.

5 FIG. 4 exemplarily illustrates a system for publishing data and the multimedia content using a client application **203** on a mobile device **202** on one or more websites simultaneously. The system disclosed herein comprises a client application **203** and a publishing service **401** connected via a network **402**. The client application **203** comprises a media publishing module **203f** as explained in the detailed description of
10 FIG. 2. The media publishing module **203f** comprises the website selection module **203g**, the timer module **203h**, the segmentation module **203i**, and the data transfer module **203j**. The website selection module **203g** selects the websites based on user preferences configured by the user on the mobile device **202**. The timer module **203h** sets the time for publishing the transferred data and the multimedia content automatically or with minimal
15 user intervention. The timer module **203h** ensures that the publishing service **401** obtains the data, the multimedia content, and the associated files to publish on the selected websites based on the time set by the user.

 In the case of limited memory and processing capabilities of the mobile device
20 **202**, the segmentation module **203i** of the client application **203** partitions the multimedia content of large files into multiple data segments. The segmentation module **203i** generates segment identifiers and tags the data segments with the segment identifiers. The segment identifiers may, for example, be one or more of transaction identifiers, sequence numbers, and timestamps. The segment identifiers are used later by a back end
25 service **401b** of the publishing service **401** to reassemble the data segments in a predetermined sequence to create a multimedia object. The data transfer module **203j** transfers the data, the tagged data segments, and the multimedia content from the client application **203** to the publishing service **401** via the network **402**. The network **402** may, for example, be a wireless network, a cellular network, or the internet **501**.

30

The publishing service **401** comprises a front end service **401a**, a back end service **401b**, and a database **401d**. The transferred data and multimedia content is stored in the database **401d** of the publishing service **401**. A protocol is provided for synchronizing user publishing information between the client application **203** and the publishing service **401**. The user publishing information may, for example, comprise user preferences of the websites and the timer setting. The data transfer module **203j** may transfer the data and the multimedia content as a single multimedia file, multiple data segments in the case of large files, or electronic mail attachments to the back end service **401b** of the publishing service **401** via the front end service **401a**. The back end service **401b** comprises a data reassembly module **401c**. If the back end service **401b** receives the multimedia content in the form of multiple data segments, the data reassembly module **401c** reassembles the data segments in a predetermined sequence using the segment identifiers. The back end service **401b** then creates a multimedia object from the transferred data and multimedia content. The multimedia object is transferred from the back end service **401b** to the front end service **401a** and then published on the websites selected by the user.

FIG. 5 exemplarily illustrates a user **502** utilizing a digital camera in conjunction with a Bluetooth enabled mobile device **202** for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. The digital camera is physically separated from the mobile device **202** as illustrated in FIG. 5. The digital camera comprises a BT communication device **201a** such as an in-built BT capability chip **301**, a BT memory card **302**, or an external BT device **303** or dongle externally attached to the digital camera as illustrated in FIGS. 3A-3C. The external BT dongle may be attached to a USB, a firewire interface, or a power port of the digital camera. The BT communication device **201a** on the digital camera is paired with the mobile device **202** to establish a connection. The user **502** may capture an image using the digital camera. The client application **203** on the mobile device **202** detects the captured image and initiates the transfer of the captured image and the associated files. The digital camera automatically transfers the captured image and the associated files to the client application **203** on the mobile device **202**.

The client application **203** automatically publishes the transferred image on one or more websites via the internet **501**. The user **502** may set preferences in the mobile device **202**. The user preferences, for example, comprise the websites selected for publishing the transferred image. The user **502** may select websites, for example, 5 Flickr™, Picasa™, YouTube™, eBay®, etc, and store the preferences on the mobile device **202**. The user **502** may also set the timer setting for publishing the transferred image on the selected websites. After the captured image is transferred to the mobile device **202**, the client application **203** publishes the capture image on the selected websites based on the default timer and website settings configured by the user **502** on 10 the mobile device **202**.

Consider an example where a user **502** records a video using a BT enabled video camera. The video camera immediately establishes a connection with the user's **502** BT enabled mobile device **202**. On detection of the recorded video by the client application 15 **203** on the mobile device **202**, the video camera automatically transfers the recorded video to the user's **502** mobile device **202**. In the case of limited memory and processing capabilities of the mobile device **202**, the recorded video may be streamed as data segments from the mobile device **202** to the publishing service **401**. The client application **203** individually tags the data segments with segment identifiers and transfers 20 the tagged data segments from the mobile device **202** to the back end service **401b** of the publishing service **401** via the front end service **401a**. The back end service **401b** of the publishing service **401** reassembles the data segments in a predetermined sequence using the segment identifiers to create the multimedia object. The multimedia object is an aggregation of the reassembled data segments. The multimedia object is then transferred 25 from the back end service **401b** to the front end service **401a** and automatically published by the front end service **401a** on one or more websites selected by the user **502**.

Consider another example where a user **502** may record videos or capture images at different points in time and automatically uploads and publishes the videos and images 30 on one or more websites. Consider an investigative reporter, Jane, working for a prominent newspaper in New York City. Each day, she moves around the city chasing

leads, interviewing people, videotaping her stories, taking pictures, and tracking down her next big story. When she is working on a story with an associate writer, she may need to upload her videos and pictures and send it immediately to the associate writer. The method and system disclosed herein enables Jane to automatically upload pictures and
5 videos taken using her digital camera or video camera onto a mobile device **202** and publish the pictures, videos, etc. from her mobile device **202** to the internet **501** with one click or touch of a button.

On one click or touch of a button, the pictures and videos are published and
10 immediately made available on Jane's private blog that may be accessed by the newspaper editor and her associates in the news office. When she is collaborating with an associate on a story, they may see each other's progress in real time. Since sharing information with the associate over electronic mails (emails) may be inconvenient, Jane records her progress on the story in the voice format and publishes. The associate may
15 access the information from Jane's blog site, thereby saving considerable time.

Exemplarily, the method and system disclosed herein may be implemented in technologies that are pervasive, flexible, and capable enough of accomplishing the desired tasks of the method and system. The method and system disclosed herein is
20 realized with, but not limited to Bluetooth communication protocol, Wireless protocols, for example, Zigbee[®] protocol, Wibree[™] protocol, Ultra-Wide Band (UWB) protocol, and other wireless protocols for wireless personal area networks may be employed to accomplish the tasks of the method and system disclosed herein. The mobile device **202** may, for example, be a ubiquitous mobile phone. The use of personal digital assistants
25 (PDAs) without telephony support is also fairly widespread. The client application **203** may be deployed on mobile devices with limited or no telephony support. These mobile devices may support Java of Sun Microsystems Inc., more specifically Java 2 Micro Edition (J2ME[™]), Windows Mobile .Net Compact Framework of Microsoft, Inc., Symbian[™], Linux framework. The client application **203** may, for example, be
30 implemented on the J2ME platform. These environments provide functionalities in the libraries to create the GUI **203e** and perform all the required functions of the method and

system disclosed herein. Other advantages of these frameworks are portability across mobile devices that run on different operating systems.

5 The client application **203** may be rendered independent of the operating system of the mobile device **202**. One of the transport mechanisms to achieve the connectivity between the publishing service **401** and the client application **203** is the wireless internet. While most PDAs have an inbuilt wireless network card for the internet connectivity, the mobile phones may transfer data to the publishing service **401** over the telephony network at near broadband speeds. Some of the mobile phones equipped with both
10 wireless network and telephony data capabilities may use either of the two to communicate with the publishing service **401**. The transport protocol that is used between the client application **203** and the publishing service **401** may be hypertext transfer protocol (HTTP) or extensible markup language-remote procedure calls (XML-RPC). The back end service **401b** may, for example, be developed in Java.

15

It will be readily apparent that the various methods and algorithms described herein may be implemented in a computer readable medium appropriately programmed for general purpose computers and computing devices. Typically a processor, for e.g., one or more microprocessors will receive instructions from a memory or like device, and
20 execute those instructions, thereby performing one or more processes defined by those instructions. Further, programs that implement such methods and algorithms may be stored and transmitted using a variety of media, for e.g., computer readable media in a number of manners. In one embodiment, hard-wired circuitry or custom hardware may be used in place of, or in combination with, software instructions for implementation of the
25 processes of various embodiments. Thus, embodiments are not limited to any specific combination of hardware and software. A "processor" means any one or more microprocessors, Central Processing Unit (CPU) devices, computing devices, microcontrollers, digital signal processors or like devices. The term "computer-readable medium" refers to any medium that participates in providing data, for example
30 instructions that may be read by a computer, a processor or a like device. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media,

and transmission media. Non-volatile media include, for example, optical or magnetic disks and other persistent memory volatile media include Dynamic Random Access Memory (DRAM), which typically constitutes the main memory. Transmission media include coaxial cables, copper wire and fiber optics, including the wires that comprise a system bus coupled to the processor. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a Compact Disc-Read Only Memory (CD-ROM), Digital Versatile Disc (DVD), any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a Random Access Memory (RAM), a Programmable Read Only Memory (PROM), an Erasable Programmable Read Only Memory (EPROM), an Electrically Erasable Programmable Read Only Memory (EEPROM), a flash memory, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read. In general, the computer-readable programs may be implemented in any programming language. Some examples of languages that can be used include C, C++, C#, or JAVA. The program will use various security, encryption and compression techniques to enhance the overall user experience. The software programs may be stored on or in one or more mediums as an object code. A computer program product comprising computer executable instructions embodied in a computer-readable medium comprises computer parsable codes for the implementation of the processes of various embodiments.

Where databases are described such as the database **401d**, it will be understood by one of ordinary skill in the art that (i) alternative database structures to those described may be readily employed, and (ii) other memory structures besides databases may be readily employed. Any illustrations or descriptions of any sample databases presented herein are illustrative arrangements for stored representations of information. Any number of other arrangements may be employed besides those suggested by, e.g., tables illustrated in drawings or elsewhere. Similarly, any illustrated entries of the databases represent exemplary information only; one of ordinary skill in the art will understand that the number and content of the entries can be different from those described herein. Further, despite any depiction of the databases as tables, other formats including

relational databases, object-based models and/or distributed databases could be used to store and manipulate the data types described herein. Likewise, object methods or behaviors of a database can be used to implement various processes, such as the described herein. In addition, the databases may, in a known manner, be stored locally or
5 remotely from a device that accesses data in such a database.

The present invention can be configured to work in a network environment including a computer that is in communication, via a communications network, with one or more devices. The computer may communicate with the devices directly or indirectly,
10 via a wired or wireless medium such as the Internet, Local Area Network (LAN), Wide Area Network (WAN) or Ethernet, Token Ring, or via any appropriate communications means or combination of communications means. Each of the devices may comprise computers, such as those based on the Intel[®] processors, AMD[®] processors, Sun[®] processors, IBM[®] processors etc., that are adapted to communicate with the computer,
15 Any number and type of machines may be in communication with the computer.

The foregoing examples have been provided merely for the purpose of explanation and are in no way to be construed as limiting of the present method and system disclosed herein. While the invention has been described with reference to various
20 embodiments, it is understood that the words, which have been used herein, are words of description and illustration, rather than words of limitation. Further, although the invention has been described herein with reference to particular means, materials and embodiments, the invention is not intended to be limited to the particulars disclosed herein; rather, the invention extends to all functionally equivalent structures, methods and
25 uses, such as are within the scope of the appended claims. Those skilled in the art, having the benefit of the teachings of this specification, may effect numerous modifications thereto and changes may be made without departing from the scope and spirit of the invention in its aspects.

1 CLAIMS

2

3 We claim:

4

5 1. A method for transferring data from a Bluetooth enabled data capture device to one or
6 more remote internet servers via a Bluetooth enabled mobile device comprising:

7

8 performing at a Bluetooth enabled data capture device:

9

10 establishing a paired Bluetooth connection between the Bluetooth enabled
11 data capture device and the Bluetooth enabled mobile device;

12

13 acquiring new data in the Bluetooth enabled data capture device, wherein
14 new data is data acquired after the paired Bluetooth connection is
15 established;

16

17 detecting and signaling the new data for transfer, to the Bluetooth enabled
18 mobile device, wherein detecting and signaling the new data for transfer
19 comprises:

20

21 receiving a request to get new data, at the Bluetooth enabled data
22 capture device, from the Bluetooth enabled mobile device, over the
23 established paired Bluetooth connection;

24

25 receiving a request to enable event notifications for new data on
26 the Bluetooth enabled data capture device, from the Bluetooth
27 enabled mobile device, over the established paired Bluetooth
28 connection;

29

30 enabling event notification on Bluetooth enabled data capture
31 device, corresponding to change in new data;

1
2 determining existence of the new data for transfer; and
3
4 sending event notification as a signal to the Bluetooth enabled
5 mobile device, corresponding to existence of new data for transfer,
6 over the established paired Bluetooth connection, wherein the
7 Bluetooth enabled mobile device listens for the event notification
8 sent from the Bluetooth enabled data capture device;
9
10 transferring the new data acquired in the Bluetooth enabled data capture to
11 the Bluetooth enabled mobile device, over the paired Bluetooth
12 connection, wherein the Bluetooth enabled mobile device has access to the
13 internet, wherein the Bluetooth enabled mobile device is configured to
14 receive the new data and send it to one or more remote internet servers.
15
16 2. The method of claim 1, wherein Bluetooth capability is provided internally in the
17 Bluetooth enabled data capture device.
18
19 3. The method of claim 1, wherein Bluetooth capability is provided to the Bluetooth
20 enabled data capture device by an external Bluetooth module.
21
22 4. The method of claim 1, wherein the new data for transfer comprises one or more of
23 audio data, video data, image data, text data, or digital data.
24
25 5. The method of claim 1, wherein event notification corresponds to creation of new
26 data for transfer or change in status of new data for transfer.
27
28 6. A method for transferring data from a Bluetooth enabled data capture device to one or
29 more remote internet servers via a Bluetooth enabled mobile device comprising:
30
31 performing at a Bluetooth enabled data capture device:

1
2 establishing a paired Bluetooth connection between the Bluetooth enabled
3 data capture device and the Bluetooth enabled mobile device;
4
5 acquiring new data in the Bluetooth enabled data capture device, wherein
6 new data is data acquired after the paired Bluetooth connection is
7 established;
8
9 detecting and signaling the new data for transfer, to the Bluetooth enabled
10 mobile device, wherein detecting and signaling the new data for transfer
11 comprises:
12
13 receiving a message from the Bluetooth enabled mobile device,
14 over the established paired Bluetooth connection, to register for
15 event notifications, corresponding to existence of new data for
16 transfer, on the Bluetooth enabled data capture device;
17
18 determining existence of the new data for transfer;
19
20 creating a new data object on the Bluetooth enabled data capture
21 device, wherein the new data object comprises new data, data
22 associated with new data and a data signal, wherein data signal is a
23 time-stamp attribute inside the data object; and
24
25 sending an event notification to the Bluetooth enabled mobile
26 device, corresponding to existence of new data for transfer, over
27 the established paired Bluetooth connection, wherein the Bluetooth
28 enabled mobile device listens for the event notification sent from
29 the Bluetooth enabled data capture device;
30

1 transferring the new data object from the Bluetooth enabled data capture
2 device to the Bluetooth enabled mobile device, over the established paired
3 Bluetooth connection, wherein the Bluetooth enabled mobile device has
4 access to the internet, wherein the Bluetooth enabled mobile device is
5 configured to receive the new data object, and send new data and time-
6 stamp to one or more remote internet servers.
7
8 7. The method of claim 6, wherein Bluetooth capability is provided internally in the
9 Bluetooth enabled data capture device.
10
11 8. The method of claim 6, wherein Bluetooth capability is provided to the Bluetooth
12 enabled data capture device by an external Bluetooth module.
13
14 9. The method of claim 6, wherein the new data for transfer comprises one or more of
15 audio data, video data, image data, text data, or digital data.
16
17 10. The method of claim 6, wherein event notification corresponds to creation of new
18 data for transfer or change in status of new data for transfer.
19
20 11. The method of claim 6, wherein the time-stamp is either absolute time or relative
21 time.
22
23 12. A method for transferring data to one or more remote internet servers by a Bluetooth
24 enabled mobile device comprising:
25
26 providing a software module on the Bluetooth enabled mobile device, wherein the
27 software module on the Bluetooth enabled mobile device is configured to perform
28 steps comprising:
29
30 establishing a paired connection between the Bluetooth enabled mobile
31 device and a Bluetooth enabled data capture device;

1
2 detecting new data acquired by the Bluetooth enabled data capture device
3 for transfer, wherein detecting the new data for transfer comprises:
4
5 sending a message to the Bluetooth enabled data capture device,
6 over the established paired Bluetooth connection, to enable event
7 notifications on the Bluetooth enabled data capture device,
8 corresponding to new data, wherein the new data is data acquired
9 by Bluetooth enabled data capture device after establishing the
10 Bluetooth pairing connection between the Bluetooth enabled data
11 capture device and the Bluetooth enabled mobile device;
12
13 enabling event notification listening on Bluetooth enabled mobile
14 device, to listen for event notifications sent from the Bluetooth
15 enabled data capture device, over the established Bluetooth
16 connection;
17
18 receiving, from the Bluetooth enabled data capture device, an
19 event notification corresponding to existence of new data for
20 transfer, over the established Bluetooth connection; and
21
22 sending a request to the Bluetooth enabled data capture device, to
23 get new data for transfer;
24
25 receiving the new data over the established Bluetooth paired wireless
26 connection, and transferring the new data received from the Bluetooth
27 enabled data capture device to one or more remote internet servers.
28
29 13. The method of claim 11, wherein the Bluetooth enabled mobile device configures the
30 new data so that it can be received by one or more remote internet servers, and

1 wherein configuring new data for receipt by one or more internet servers comprises
2 specifying action setting and destination address of one or more internet servers.

3
4 14. The method of claim 11, wherein the new data for transfer comprises one or more of
5 audio data, video data, image data, text data, or digital data.

6
7 15. The method of claim 11, wherein event notification corresponds to creation of new
8 data for transfer or change in status of new data for transfer.

9
10 16. A method for transferring data to one or more remote internet servers by a Bluetooth
11 enabled mobile device comprising:

12
13 performing at a Bluetooth enabled mobile device:

14
15 establishing a paired connection between the Bluetooth enabled mobile
16 device and a Bluetooth enabled data capture device;

17
18 detecting new data acquired by the Bluetooth enabled data capture device
19 for transfer, wherein detecting the new data for transfer comprises:

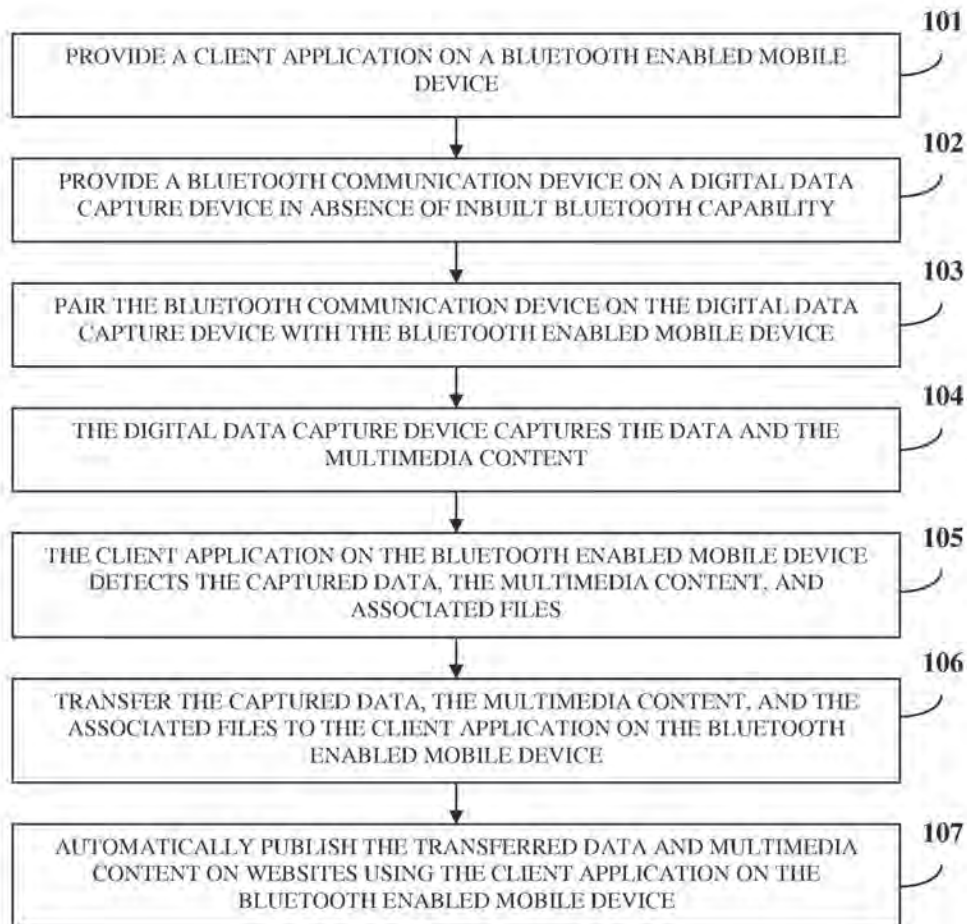
20
21 sending a message to the Bluetooth enabled data capture device,
22 over the established paired Bluetooth connection, to enable event
23 notifications on the Bluetooth enabled data capture device,
24 corresponding to new data, wherein the new data is data acquired
25 by Bluetooth enabled data capture device after establishing the
26 Bluetooth pairing connection between the Bluetooth enabled data
27 capture device and the Bluetooth enabled mobile device;

28
29 enabling event notification listening on the Bluetooth enabled
30 mobile device, to listen for event notifications sent from the

1 Bluetooth enabled data capture device, over the established
2 Bluetooth connection;
3
4 receiving, from the Bluetooth enabled data capture device, an
5 event notification corresponding to existence of new data for
6 transfer, over the established Bluetooth connection; and
7
8 sending a request to the Bluetooth enabled data capture device, to
9 get new data object for transfer, wherein new data object
10 comprises of new data, data associated with new data and time-
11 stamp;
12
13 receiving the new data object over the established Bluetooth paired
14 wireless connection, and sending new data and time-stamp to one or more
15 remote internet servers.
16
17 17. The method of claim 15, wherein the Bluetooth enabled mobile device configures the
18 new data so that it can be received by one or more remote internet servers, and
19 wherein configuring new data for receipt by one or more internet servers comprises
20 specifying action setting and destination address of one or more internet servers.
21
22 18. The method of claim 15, wherein the new data for transfer comprises one or more of
23 audio data, video data, image data, text data, or digital data.
24
25 19. The method of claim 15, wherein event notification corresponds to creation of new
26 data for transfer or change in status of new data for transfer.
27
28 20. The method of claim 15, wherein the time-stamp is either absolute time or relative
29 time.
30
31

ABSTRACT

Disclosed herein is a method and system for utilizing a digital data capture device in conjunction with a Bluetooth (BT) enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. A client application is provided on the BT enabled mobile device. In the absence of inbuilt BT capability, a BT communication device is provided on the digital data capture device. The BT communication device is paired with the BT enabled mobile device to establish a connection. The client application detects capture of data and multimedia content on the digital data capture device and initiates transfer of the captured data, multimedia content, and associated files. The digital data capture device transfers the captured data, multimedia content, and the associated files to the client application. The client application automatically publishes the transferred data and multimedia content on one or more websites.

**FIG. 1**

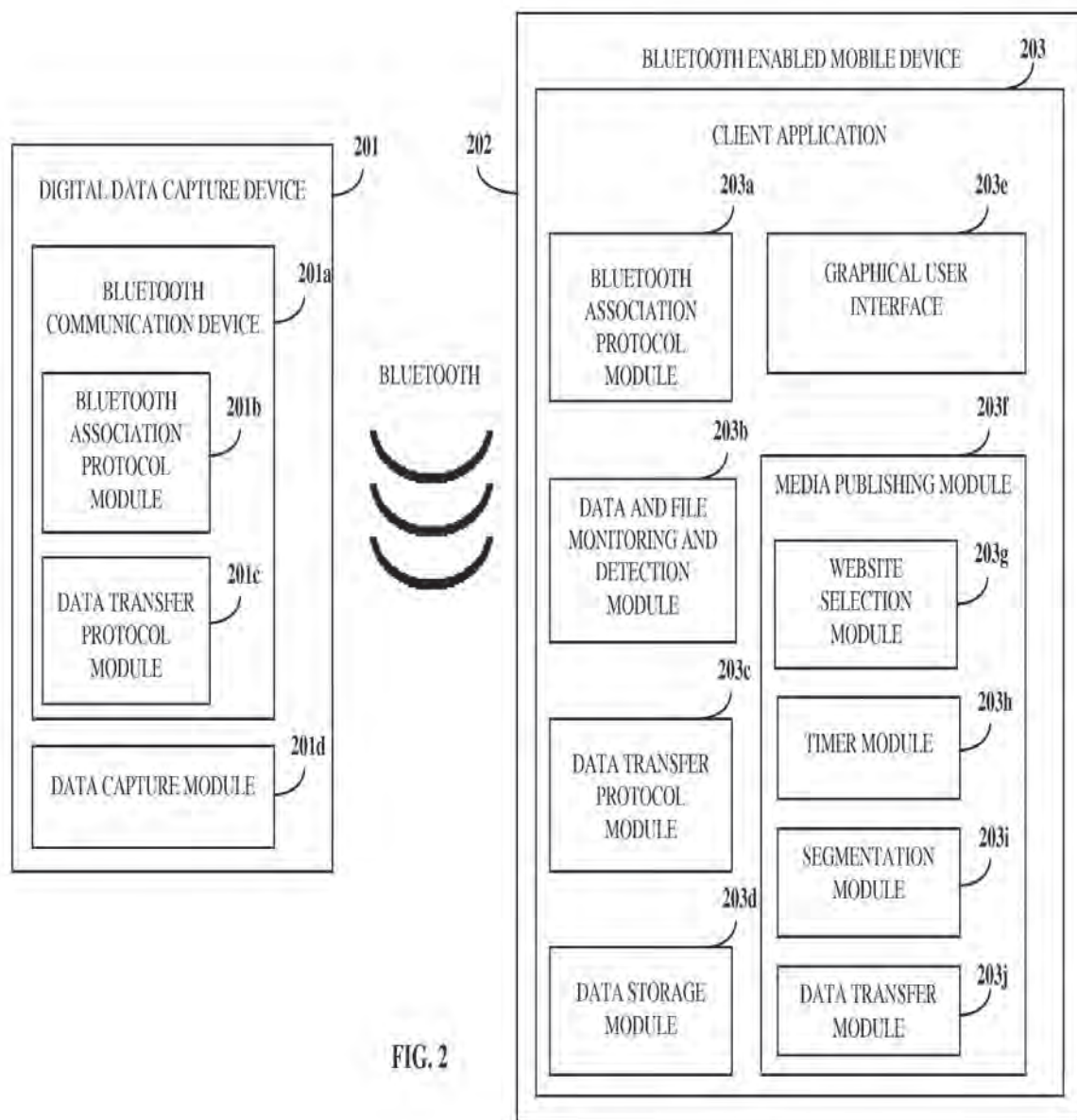


FIG. 2

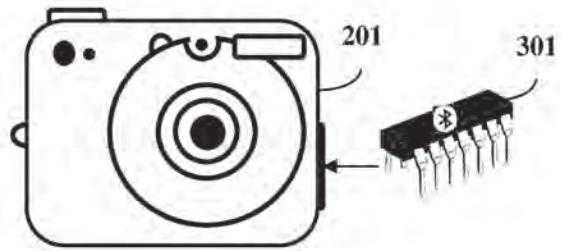


FIG. 3A

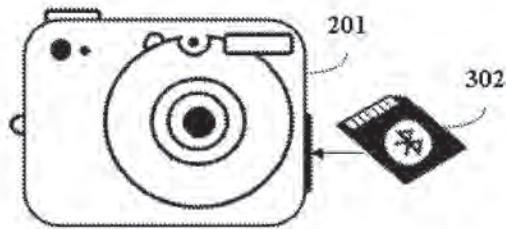


FIG. 3B

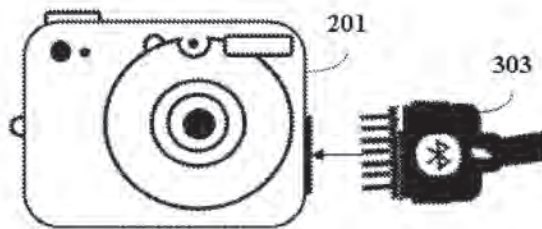


FIG. 3C

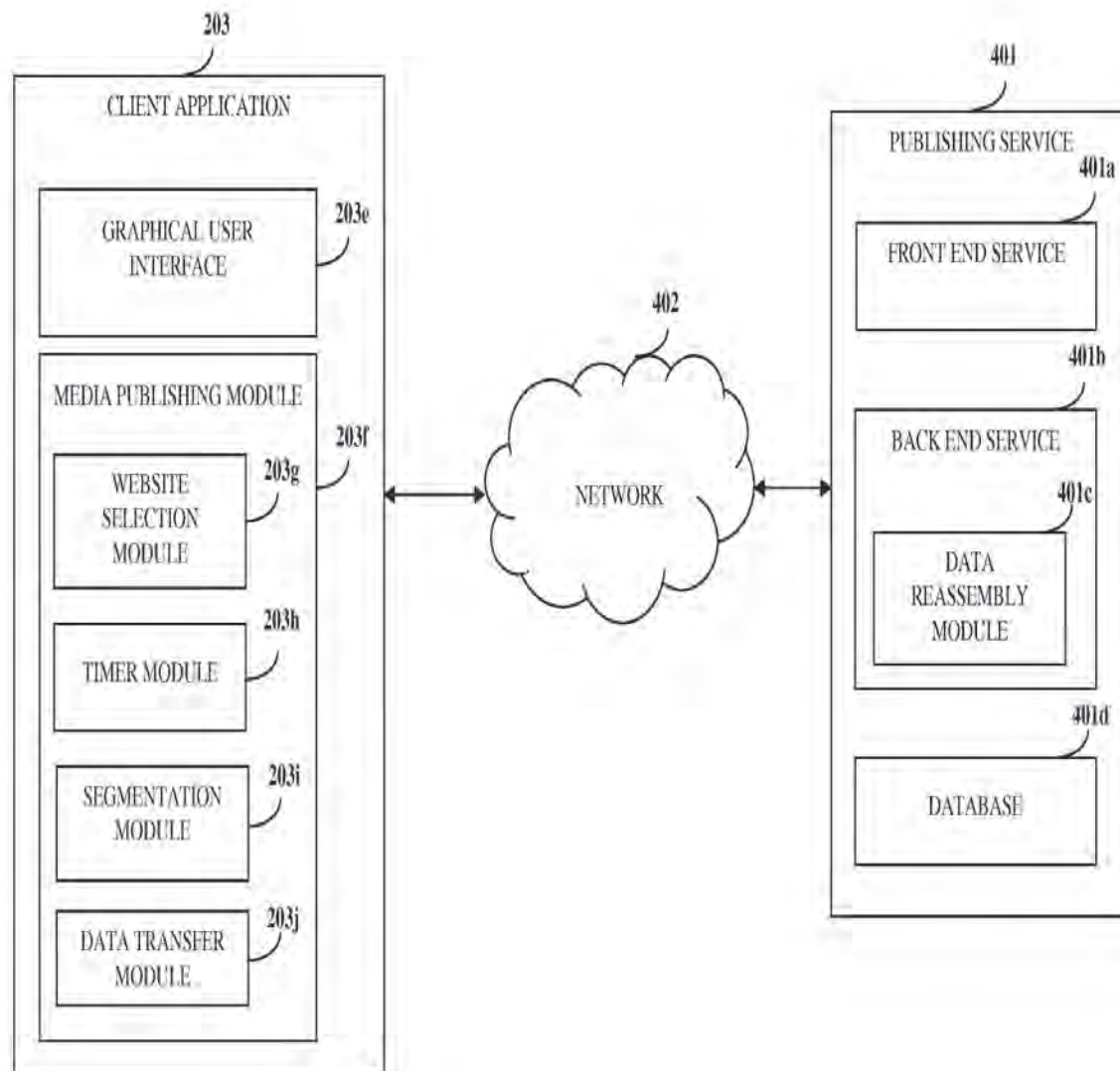


FIG. 4

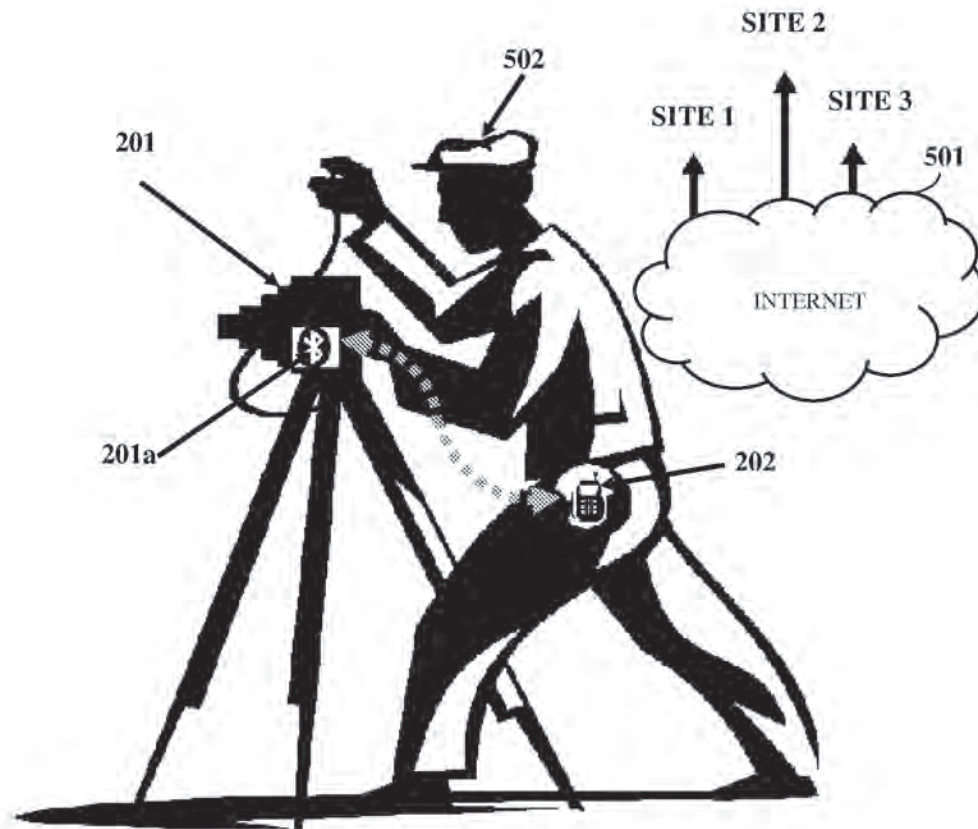


FIG. 5